**January 22, 2001**

**INSPECTOR GENERAL MANUAL 5200.1**

# INFORMATION SECURITY PROGRAM MANUAL

## FOREWORD

This Manual prescribes policy and assigns responsibility to facilitate the effective and uniform application of the DoD Information Security Program within the Office of the Inspector General, Department of Defense (OIG, DoD). The Manual supplements DoD 5200.1-R, "Information Security Program," January 1987, by amplifying the basic DoD policies contained therein and by providing policy guidance, where appropriate, for application within the OIG, DoD.

The Manual contains information as listed in DoD 5200.1-R and should be used in conjunction with that regulation to obtain complete guidance on a specific security topic or subject. Where DoD 5200.1-R provides sufficient guidance, no OIG, DoD, supplementation will be furnished. The Manual provides additional instructions that are not covered by DoD 5200.1-R, but are related to the OIG, DoD, security program.

As amended by Executive Order (E.O.) 13142, November 19, 1999, E.O. 12958, "Classified National Security Information," April 17, 1995, effective October 14, 1995, has been incorporated into this Manual. In cases of conflict between the E.O. and DoD 5200.1-R, the E.O. takes precedence.

Recommended changes to this Manual must be forwarded through appropriate channels to the Office of Administration and Information Management, Attention: Administrative Services Division.

This Manual is effective immediately.

FOR THE INSPECTOR GENERAL:

//Signed//
Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

# TABLE OF CONTENTS

**Page**

## Chapter 1. General


1.1. Purpose ..... 1-1
1.2. References ..... 1-1
1.3. Cancellation ..... 1-1
1.4. Applicability ..... 1-1
1.5. Definitions ..... 1-1
1.6. Authority ..... 1-1
1.7. Policy ..... 1-1
1.8. Responsibilities ..... 1-1
1.9. Procedures ..... 1-1
1.10. Executive Order Overview ..... 1-1
1.11. Delegation of Authority ..... 1-3


## Chapter 2. Classification Management

### Section 1
### Classification and Original Classification Authority


2.1. Background ..... 2-1
2.2. Authority ..... 2-1
2.3. Delegated Responsibility ..... 2-1
2.4. Senior Official for Information Security ..... 2-1
2.5. Classification Categories ..... 2-2
2.6. Classification Levels ..... 2-2
2.7. Classification Standards ..... 2-2
2.8. Responsibilities of Classifiers ..... 2-3


### Section 2
### Markings


2.9 Identifying and Marking Classified Information ..... 2-4
2.10. Identification of Authorities ..... 2-4
2.11. Overall Markings ..... 2-4
2.12. Portion Marking ..... 2-4
2.13. Classification Extensions ..... 2-5
2.14. Marking Information Exempted From Automatic Declassification at 25 Years ..... 2-5
2.15. Derivative Classification Markings ..... 2-6
2.16. Overall Marking (Derivative) ..... 2-7
2.17. Portion Marking (Derivative) ..... 2-7
2.18. Marking Prohibitions ..... 2-7
2.19. Transmittal Document ..... 2-7
2.20. Foreign Government Information ..... 2-8
2.21. Working Papers ..... 2-8
2.22. Bulky Material ..... 2-8
2.23. Unmarked Presidential Materials ..... 2-8
2.24. Distribution Controls ..... 2-8
2.25. Specific Marking on Documents ..... 2-8

2.26. Overall and Page Markings ..... 2-8
2.27. File, Folder, or Group of Documents ..... 2-9
2.28. Markings on Special Categories of Material ..... 2-9
2.29. Miscellaneous Material ..... 2-9
2.30. For Official Use Only (FOUO) ..... 2-9

**Section 3**
**Classification Prohibitions and Limitations**

2.31. Classification Prohibitions ..... 2-11
2.32. Classification Challenges ..... 2-11
2.33. Classification Challenge Tracking System ..... 2-11
2.34. Classification Challenge Review Process ..... 2-12
2.35. Reevaluation of Classification Because of Compromise ..... 2-12

**Section 4**
**Classification Guides**

2.36. Classification Guides ..... 2-13

**Section 5**
**Declassification and Downgrading**

2.37. Declassification and Downgrading ..... 2-14
2.38. Automatic Declassification ..... 2-14
2.39. Systematic Declassification ..... 2-15
2.40. Mandatory Declassification Review ..... 2-15
2.41. Processing Requests and Reviews ..... 2-15

## Chapter 3. Safeguarding

**Section 1**
**Safekeeping and Storage**

3.1. General Policy ..... 3-1
3.2. Standards for Storage Equipment ..... 3-1
3.3. Storage of Classified Information ..... 3-1
3.4. Replacement of Combination Locks ..... 3-1
3.5. Storage of Bulky Material ..... 3-2
3.6. Key Accountability ..... 3-2
3.7. Procurement of New Storage Equipment ..... 3-2
3.8. Numbering and Designating Storage Facilities ..... 3-2
3.9. Combinations to Containers and Vaults ..... 3-2
3.10. Repair of Damaged Security Containers ..... 3-3
3.11. Moving/Turn-in of Safes ..... 3-3

**Section 2**
**Custodial Precautions**

3.12. Responsibilities of Custodians ..... 3-6
3.13. Residential Storage Arrangements ..... 3-6
3.14. Care During Working Hours ..... 3-6
3.15. End-of-Day Security Checks ..... 3-7

3.16. Emergency Planning ..... 3-8
3.17. Telecommunications Conversations ..... 3-8
3.18. Removal of Classified Storage and Information Processing Equipment ..... 3-8
3.19. Classified Discussions, Meetings, and Conferences ..... 3-8
3.20. Safeguarding U.S. Classified Information Located in Foreign Countries ..... 3-9
3.21. Non-COMSEC Classified Information Processing Equipment ..... 3-10

## Chapter 4. Classified Document Control

### Section 1
### Access

4.1. General Restrictions on Access ..... 4-1
4.2. Policy ..... 4-1

### Section 2
### Dissemination

4.3. Policy ..... 4-6
4.4. Special Requirements for Release of Classified Intelligence Information to DoD Contractors ..... 4-6

### Section 3
### Accountability and Control

4.5. Collateral Top Secret Control Officer Program ..... 4-8
4.6. Accountability ..... 4-8
4.7. Top Secret Registers ..... 4-8
4.8. Inventory ..... 4-8
4.9. Secret and Confidential Information ..... 4-9
4.10. Working Papers ..... 4-9
4.11. North Atlantic Treaty Organization (NATO) and Joint Chiefs of Staff (JCS) Documents ..... 4-10
4.12. Receipts ..... 4-10

### Section 4
### Reproduction

4.13. Restraint on Reproduction ..... 4-13
4.14. Key Operators ..... 4-13
4.15. Designation of Copiers ..... 4-13
4.16. Facsimile Machine Controls ..... 4-13

## Chapter 5. Transmission

### Section 1
### Methods of Transmission or Transportation

5.1. Policy ..... 5-1
5.2. Top Secret Information ..... 5-1
5.3. Secret and Confidential Information ..... 5-1

5.4. Accountable Mail ..... 5-2
5.5. Transmission of Classified Material to Foreign Governments ..... 5-2

**Section 2**
**Preparation of Material for Transmission, Shipment, or Conveyance**

5.6. Envelopes or Containers ..... 5-4
5.7. Addressing ..... 5-4
5.8. Receipt System/SD Form 120 ..... 5-4

**Section 3**
**Restrictions, Procedures, and Authorization Concerning Escort or Hand Carrying of Classified Information**

5.9. General Restrictions ..... 5-7
5.10. Approval Process ..... 5-7
5.11. Procedures for Hand Carrying Classified Information Aboard Commercial Passenger Aircraft ..... 5-7

## Chapter 6. Disposal and Destruction

6.1. Policy ..... 6-1
6.2. Destruction of Material ..... 6-1
6.3. Annual Clean-Out Day ..... 6-2

## Chapter 7. Security Education

7.1. Responsibility and Objectives ..... 7-1
7.2. Scope and Principles ..... 7-1
7.3. Security Education ..... 7-1

## Chapter 8. Compromise of Classified Information

8.1. Policy ..... 8-1
8.2. Purpose of Inquiry or Investigation ..... 8-1
8.3. Debriefings in Cases of Unauthorized Access ..... 8-1
8.4. Responsibility of Discoverer ..... 8-2
8.5. Appointment of Preliminary Inquiry Officer (PIO) ..... 8-2
8.6. Handling Instructions ..... 8-3

## Chapter 9. Information Systems

9.1. Background ..... 9-1
9.2. General Requirements ..... 9-1
9.3. Certification and Accreditation Overview ..... 9-1
9.4. Overview of Modes of Operation ..... 9-1
9.5. Additional Security Concerns ..... 9-2
9.6. Physical Security ..... 9-2

9.7. Personnel Security ..... 9-2
9.8. Accountability, Marking, and Control of Information Systems Media ..... 9-2
9.9. Storage Media Review ..... 9-3
9.10. Violations and Compromise ..... 9-3

## Chapter 10. North Atlantic Treaty Organization (NATO) Classified Information

10.1. NATO Classified Information ..... 10-1

## Chapter 11. Program Management

11.1. General Management ..... 11-1
11.2. Program Monitoring ..... 11-1
11.3. Field Program Management ..... 11-1
11.4. Appointing Authorities ..... 11-1
11.5. Appointed Security Managers ..... 11-2

## Chapter 12. Building Entrance Policy/Badges/ Property Passes/Escorting

12.1. Policy ..... 12-1
12.2. Basic Rules for Escorting and General Escort Requirements ..... 12-2
12.3. Escorting Persons with a Suspended Clearance or Restricted Access ..... 12-2
12.4. Non-receipt of Visit Certification Letter ..... 12-2
12.5. Field Activity Managers and OIG Components ..... 12-2
12.6. Challenges ..... 12-3

## Chapter 13. OIG Self Inspection Program

Program Management ..... 13-1
Classification Management ..... 13-2
Document Marking ..... 13-2
Safeguarding and Storage ..... 13-3
Reproduction of Classified Material ..... 13-5
Disposition and Destruction of Classified Material ..... 13-5
Transmission and Transportation of Classified Information ..... 13-5
Security Education ..... 13-6
Security Incidents and Violations, to Include Compromises ..... 13-7

## Appendices

A References ..... A-1
B Definitions ..... B-1

## Figures


1 Sample Standard Form 706, 707, 708, 709, 710, and 711 ..... 2-10
2 Sample Standard Form 700, Security Container Information ..... 3-5
3 Sample Classified Cover Sheets, SF 703, 704, and 705 ..... 3-11
4 Sample Optional Form 23, Charge Out Record ..... 3-12
5 Sample Standard Form 702, Security Container Check Sheet ..... 3-13
6 Sample Standard Form 701, Activity Security Checklist ..... 3-14
7 Sample Standard Form 312, Classified Information Non-Disclosure Agreement ..... 4-4
8 Sample Visit Request Letter ..... 4-5
9 Sample IG Form 5200.1-8, Top Secret Register Page ..... 4-11
10 Sample IG Form 5200.1-5, Top Secret Access Record and Cover Sheet ..... 4-12
11 Sample IG Form 5200.1-1, Authorization for Reproduction of Classified Material ..... 4-15
12 Sample DD Form 2501, Courier Authorization ..... 5-3
13 Sample SD Form 120, OSD Receipt for Classified Material ..... 5-6
14 Sample Request for Approval to Escort or Hand Carry Classified Information Aboard Commercial Passenger Aircraft ..... 5-9
15 Sample Courier Authorization Letter ..... 5-11
16 Sample IG Form 5200.1-10, Classified Material Destruction Certificate ..... 6-3
17 Sample IG Form 5200.1-23, Burn Bag Receipt ..... 6-4
18 Sample IG Form 5200.2-1, Security Termination Statement ..... 7-3
19 Sample Optional Form (OF) 7, Property Pass ..... 12-4

# CHAPTER 1
# GENERAL

**1.1. Purpose.** This Manual prescribes policy and assigns responsibility to facilitate the effective and uniform application of the DoD Information Security Program within the Office of the Inspector General, Department of Defense (OIG, DoD).

**1.2. References.** See Appendix A.

**1.3. Cancellation**. This Manual cancels IGDM 5200.1, *Information Security Program Manual*, dated August 1, 1988.

**1.4. Applicability**. This Manual applies to the Office of the Inspector General; the Deputy Inspector General; Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; and Director, Intelligence Review (hereafter referred to as OIG components) and all field offices.

**1.5. Definitions.** See Appendix B.

**1.6. Authority.** This Manual is published in accordance with:

a. Executive Order (E.O.) 12958, "Classified National Security Information," April 17, 1995, effective October 14, 1995 (reference a).

b. DoD 5200.1-R, "Information Security Program," January 17, 1997 (reference b).

**1.7. Policy**

a. Each individual who possesses or who has knowledge of such information regardless of how it was obtained will protect classified information.

b. Compliance with the provisions of this Manual is mandatory. Violators are subject to administrative or judicial sanctions, or both.

c. Additional policy regarding information security is prescribed throughout pertinent chapters of this Manual.

**1.8. Responsibilities.** All OIG managers are responsible for the effective application of information security policies and procedures within their organization. They must ensure that individuals who have access to classified information are appropriately cleared, are aware of their security responsibilities, and are indoctrinated and proficient in the security policy and procedures that apply to them in the performance of their duties. Additional responsibilities for security managers and individuals are listed elsewhere in this Manual.

**1.9. Procedures.** Procedures for implementing security guidelines are provided in reference b and this Manual.

**1.10. E.O. Overview.** Reference a prescribes a uniform system for managing the protection of national security information. Highlights of the E.O. are listed below:

a. Discourages unnecessary classification by instructing classifiers to keep information unclassified when in doubt and directs classifiers to choose the lower level of classification when in doubt about which level is appropriate.

b. Limits the duration of classification of most newly classified information to 10 years, subject to limited exceptions.

c. Mandates automatic declassification of information that is 25 years old, unless it falls within one of the narrow exemption categories, such as revealing the identity of a human source.

d. Establishes an Interagency Security Classification Appeals Panel to hear appeals of agency decisions on mandatory declassification review requests or challenges to classification and to review an agency head's determination to exempt 25-year-old information from automatic declassification.

e. Authorizes agency officials to determine whether the public interest in disclosure outweighs the national security interest in maintaining classification when deciding whether to declassify information that otherwise continues to meet the standards for classification.

f. Implements a number of management improvements to better safeguard classified information and reduce the overall costs of protecting such information.

g. Stresses a general commitment to openness as a part of the classification management process.

h. Requires classifiers to identify why information is classified.

i. Eliminates the presumption that any category of information is automatically classified.

j. Specifies sanctions for over-classification.

k. Requires the establishment of a Government-wide declassification database.

l. Establishes an Information Security Policy Advisory Council of non-Government experts to recommend subject areas for systematic declassification review and to advise on classification system policies.

m. Limits the establishment and requires annual revalidation of Special Access Programs (SAPs) and increases both internal and external oversight of these programs.

n. Requires accounting and reporting of costs associated with security classification program.

o. Mandates training and accountability of Original Classification Authorities (OCAs).

p. Calls for challenges of improper classification decisions and establishes processing procedures to ensure non-retribution.

q. Requires personal commitment of OIG Component Heads and senior management to the effective implementation of the system.

r. Requires that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(1) OCAs.
(2) Security managers or security specialists.

(3) All other personnel whose duties significantly involve the creation or handling of classified information.

**1.11. Delegation of Authority.** The Director for Administration and Information Management (OA&IM) has delegated to the Director, Personnel and Security, the responsibility for implementation and compliance with DoD regulations and for the establishment and administration of the OIG Information Security Program. The OIG Security Division will apprise the Director, Personnel and Security, of the security posture of the OIG, DoD, and the status of ongoing investigations into security infractions and violations.

# CHAPTER 2
# CLASSIFICATION MANAGEMENT

## SECTION 1
## CLASSIFICATION AND ORIGINAL CLASSIFICATION AUTHORITY

**2.1. Background.** Reference a prescribes a uniform system for classifying, safeguarding, and declassifying national security information assigned to keep the American people informed on the activities of Government. The E.O. also protects information critical to our nation's security. Implementing guidance on the provisions of reference a are contained in the Information Security Oversight Office (ISOO) directives. Reference b implements reference a.

**2.2. Authority.** Under the authority delegated in reference a, the Inspector General may exercise and delegate to principal subordinate officials the authority to originally classify national security information as Secret and Confidential. The Inspector General has designated the Director, Personnel and Security, as the Senior Official for Information Security. Each delegation of original classification authority will be recorded, and such authority shall not be redelegated.

**2.3. Delegated Responsibility.** The Inspector General has been delegated Top Secret Original Classification Authority for this agency. Requests for additional delegation of original Top Secret classification authority, with appropriate justification, shall be submitted through proper channels for approval by the Secretary of Defense. Similarly, requests for additional original Secret and Confidential classification authority shall be submitted to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), for approval.

**2.4. Senior Official for Information Security.** The Director, Personnel and Security, is responsible for actively overseeing the OIG, DoD, information security program, including a security education program, to ensure effective implementation of reference a. These responsibilities include establishing and monitoring policies and procedures to prevent over or under-classification of national security information and protecting classified information from unauthorized disclosure. The Senior Official for Information Security will recommend the following to the Inspector General:

a. Proposals for reclassification in accordance with reference a.

b. Implementation plans that protect classified information and prevent unauthorized disclosure.

c. Identification of those officials, by position, delegated as Secret and/or Confidential classification authority.

d. Guidance concerning corrective or disciplinary action in unusually important cases involving unauthorized disclosure.

e. Reporting to the ISOO information and reports required under reference a.

f. Systematic document review for early downgrading, declassification, and public availability.

g. Reduction of the amount of classified material and the number of persons authorized to classify.

h. Establishment and implementation of a system for processing, tracking, and recording formal classification challenges made by authorized holders.

i. Guidance on agency development and implementation of an automatic declassification plan.

j. Training for all original and derivative classification authorities in classification, as provided in reference a and its implementing directives.

## 2.5. Classification Categories

a. To qualify for classification, information must meet two tests. First, it must fall under one of the specified classification criteria listed below (Section 1.5 of reference a). Second, an official with original classification authority must determine whether the unauthorized disclosure of the information, either by itself or in the context of other information, could reasonably be expected to cause damage to the national security.

b. Information may not be considered for classification unless it concerns:

**(Extracts from E.O. 12958, Section 1.5. Classification Categories)**

(1) Sec 1.5 a. Military plans, weapons systems or operations;
(2) Sec 1.5 b. Foreign government information;
(3) Sec 1.5 c. Intelligence activities, sources, methods, or cryptology;
(4) Sec 1.5 d. Foreign relations or foreign activities of the United States, including confidential sources;
(5) Sec 1.5 e. Scientific, technological or economic matters relating to the national security;
(6) Sec 1.5 f. United States programs for safeguarding nuclear materials or facilities; or
(7) Sec 1.5 g. Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security.

**2.6. Classification Levels.** Information may be classified at one of the following three levels:

a. TOP SECRET - Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

b. SECRET - Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

c. CONFIDENTIAL - Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

d. Except as otherwise provided by statute, no other terms shall be used to identify United States classified information. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

**2.7. Classification Standards.** Information may be originally classified under the terms of reference a only if all of the following conditions are met:

a. An original classification authority is classifying the information.

b. The information is owned by, produced by or for, or is under the control of the United States Government.

c. The information falls within one or more of the categories of information listed in section 1.5 of reference a.

d. The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

e. If there is significant doubt about the need to classify information, it shall not be classified. Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

**2.8. Responsibilities of Classifiers.** Classifiers are responsible for proper classification and protection of documents that they create. Information is classified in one of two ways - originally and derivatively. Only Original Classification Authority (OCA), may formally make original classification determinations. Individuals with a security clearance, who are required by their work to restate classified information from an already classified source document may classify derivatively at the level of their clearance. Classifiers must determine which information is classified as SECRET or CONFIDENTIAL (depending on the classification authority delegated to that individual), how long it needs to be protected and properly mark that information.

# CHAPTER 2
# CLASSIFICATION MANAGEMENT

## SECTION 2
## MARKINGS

**2.9. Identifying and Marking Classified Information.** A uniform security classification system requires that standard markings be applied to classified information. Except in extraordinary circumstances or as indicated in this Manual and in references a, b, and c, the marking of classified information created after October 16, 1995, shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information, the originator shall provide holders or recipients of the information with written instructions for protecting the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required and the duration of classification. The overall marking must be conspicuous enough to alert anyone handling the document that it is classified. If the markings do not attract your attention, it is not conspicuous. Overall, classification markings must be larger and **Bolder** than other text on the page.

**2.10. Identification of Authorities.** The face of each originally classified document shall bear the following:

a. Classification Authority. The name or personal identifier and position title of the original classifier shall appear on the "Classified By" line. For example:

Classified By: John Doe, Chief, Division 5

b. Agency and Office of Origin. If not otherwise evident, the agency and office of origin shall be identified and placed below the "Classified By" line. For example:

Classified By: John Doe, Chief, Division 5
Department of Good Works, Office of Administration

c. Reason for Classification. The original classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category in section 1.5 of reference a. For example:

Reason: 1.5 (b), (c), & (g).

**2.11. Overall Marking.** The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the information text.

a. Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page and on the outside of the back cover (if any).

b. For documents comprised of information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked "SECRET" and other information marked "CONFIDENTIAL," the overall marking would be "SECRET."

**2.12. Portion Marking.** Each portion of a document, usually a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

a. To indicate the appropriate classification level, the symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used.

b. Waivers from the portion marking requirements for a specific category of information must be forwarded through the OIG Security Division before submission to the ISOO for final approval. All requests must include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver by the ISOO.

**2.13. Classification Extensions.** An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. For information contained in records determined to be permanently valuable, multiple extensions shall not exceed 25 years from the date of origin of the information. The "Declassify On" line shall indicate the date the original declassification instructions have changed. The revised instructions shall be conspicuously applied to the face of the document and shall include the identity of the person authorizing the extension or other revision. The office of origin shall make reasonable attempts to notify all holders of such information and classification guides shall be updated to reflect such revisions. An example of an extended duration of classification made on October 16, 2005, and originally marked for declassification 10 years from the date of the decision, may appear as follows:

Classified By: John Doe, Chief, Division 5
Department of Good Works, Office of Administration
Reason:1.5(g)
Declassify On: ~~October 16, 2005~~
Classification extended until October 16, 2015
by: John Doe, Chief, Division 5

**2.14. Marking Information Exempted From Automatic Declassification at 25 Years.** When an OIG, DoD, senior official exempts permanently valuable information from automatic declassification at 25 years, the "Declassify On" line shall be revised to include the symbol "25X" plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) in section 3.4(b) of reference a. Other than when the exemption pertains to the identity of a confidential source, or a human intelligence source, the revised "Declassify On" line shall also include the new date or event for declassification. These categories are:

**(Extracted from Executive Order 12958)**

25X1: Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States.

25X2: Reveal information that would assist in the development or use of weapons of mass destruction.

25X3: Reveal information that would impair U.S. cryptologic systems or activities.

25X4: Reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system.

25X5: Reveal actual U.S. military war plans that remain in effect.

25X6: Reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States.

25X7: Reveal information that would clearly and demonstrably impair the current ability of U.S. Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized.

25X8: Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans.

25X9: Violate a statute, treaty or international agreement.

The pertinent portion of the marking might appear as follows:

Declassify On: 25X-State-of-the-art technology within U.S. weapons system.
October 1, 2010
or
Declassify On: 25X4
October 1, 2010

**2.15. <u>Derivative Classification Markings</u>.** Information classified derivatively based on source documents or classification guides will bear all markings except as provided below. Information for these markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

a. **"Derived From" Line.** "Classified By" line is replaced with a "Derived From" line. The "Reason" line, as reflected in the source document(s) or classification guide, is not required to be transferred to the derivative document. The derivative classifier shall concisely identify the source document or the classification guide on this line, including the agency and office of origin. For example:

Derived From: John Doe, Chief, Division 5
Department of Good Works, Office of Administration
Memo dated October 20, 1995
or
Derived From: CG No.1, Department of Good Works,
dated October 20, 1995

b. **More Than One Source Document.** When a document is classified derivatively based on <u>more than one source document</u> or <u>classification guide</u>, the "Derived From" line shall appear as follows:

Derived From: Multiple Sources

(1) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document**.**

(2) A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" shall cite the source documents on its "Derived From" line rather than the term "Multiple Sources." For example:

Derived From: Report entitled, "New Weapons,"
dated October 20, 1995,

Department of Good Works,
Office of Administration

c. **Reason for Classification.** The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not required to be transferred in a derivative classification action.

d. **Declassification Instructions.** The derivative classifier shall carry forward the "Declassify On" line from the source document to the derivative document, or the duration instructions from the classification guide. When a document is classified derivatively based on more than one source document or classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources.

(1) When a document is classified derivatively from a source document or classification guide that contains the declassification instructions, "Originating Agency Determination Required," or "OADR," unless otherwise instructed by the original classifier, the derivative classifier shall carry forward:

(a) The fact that the source document(s) was marked with this instruction and the date of origin of the source document(s) or classification guide.

An example might appear as follows:
Declassify On: Source marked "OADR"
Date of Origin: October 20, 1990

(b) This marking will permit the determination of when the classified information is 25 years old and, if permanently valuable, subject it to automatic declassification under section 3.4 of reference a.

**2.16. Overall Marking (Derivative).** The derivative classifier shall carry forward the overall marking from the source document or the classification level instruction from the classification guide and mark the derivative document as provided above. When a document is classified derivatively based on more than one source document or classification guide, the overall marking shall reflect the highest level of classification of any its sources.

**2.17. Portion Marking (Derivative).** Each portion of a derivatively classified document shall be marked in accordance with its source and as indicated above.

**2.18. Marking Prohibitions.** Markings other than "Top Secret," "Secret," or "Confidential" shall not be used to identify information as classified national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify classified national security information. The terms "Top Secret," "Secret," and "Confidential" may not be used to identify unclassified executive branch information. Classifiers will refrain from the use of special markings when they merely restate or emphasize the principles and standards of reference a. Any special markings used outside the scope of reference a must receive prior approval from the Director, ISSO.

**2.19. Transmittal Document**. A transmittal document shall indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal letter will include the highest overall marking of the document and if the transmittal contains no classified information in the body of the letter, the following statement will be centered at the bottom of the page.

**UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE REMOVED**

*(OR, if classified information is contained in the body of the letter)*

**UPON REMOVAL OF ATTACHMENTS, THIS DOCUMENT IS (*CLASSIFICATION*)**

**2.20. Foreign Government Information (FGI).** Documents that contain foreign government information shall include either the marking "Foreign Government Information," "FGI" or a marking that otherwise indicates that the information is of foreign origin. If the fact that information is foreign government information must be concealed, the marking will not be used and the document shall be marked as if it were wholly of U.S. origin.

**2.21. Working Papers.** Working papers containing classified information will be dated when created, marked with the highest classification of any information contained in them, protected at that level, and destroyed when no longer needed. When any of the following apply, working papers will be controlled and marked in the same manner prescribed for a finished document at the same classification level:

a. Released by the originator outside of the originating activity.

b. Retained more than 180 days from date of origin.

c. Filed permanently.

**2.22. Bulky Material**. Bulky material, equipment, and facilities, etc., will be clearly identified in a manner that leaves no doubt about the classified status of the material, the level of protection required and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding must be maintained in the appropriate security facility and in any applicable classification guide.

**2.23. Unmarked Presidential Materials.** Information contained in unmarked presidential or related materials preserved in a presidential library or other repository and which pertains to the national defense or foreign relations of the United States and has been maintained and protected as classified information under prior orders shall continue to be treated as classified information under reference a, and is subject to its provisions regarding classification.

**2.24. Distribution Controls.** Each OIG component will maintain control over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need to know the information. All recipients will cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in document status occurs.

**2.25. Specific Marking on Documents.** Reference c provides illustrated guidance on the application of original/derivative classification and associated markings to documents prepared by the DoD. The OIG, DoD, personnel are encouraged to use this document as a general guide. Reference b should be referred to when using special intelligence markings.

**2.26. Overall and Page Markings.** At the time of original/derivative classification, the document shall be marked in capital letters (preferably in red ink) at the top and bottom of the title/first page with the overall classification of the document and at the top and bottom of each interior page with the highest classification of information on the page. Within a classified document, the top and bottom of each page that contains no classified information shall be marked "Unclassified" or "For Official Use Only," as appropriate (preferably in black ink).

**2.27. File, Folder, or Group of Documents.** When classified information is permanently filed (bound or unbound) in a folder, the folder shall be marked in capital letters (preferably in red ink) at the top and bottom (front and back) with the highest classification of information contained in the folder. When possible, the top front marking on the folder used for filing classified material shall be accomplished in a manner that allows the classification to remain visible once the folders have been filed.

**2.28. Markings on Special Categories of Material.** Standard Form (SF) 706, "Top Secret Label, SF 707, "Secret Label," and SF 708, "Confidential Label," are color-coded adhesive labels that shall be used, whenever possible, when marking special categories of classified material (i.e., non-document material, such as typewriter ribbons and the like). SF 709, "Classified," SF 710, "Unclassified," and SF 711, "Data Descriptor Label," also adhesive labels, shall be used in conjunction with SF 706, 707, and 708, whenever possible, when applying any necessary additional identifying data and/or safeguarding procedures (e.g., "NATO") to special categories of material. (See sample labels at Figure 1, page 2-10.)

**2.29. Miscellaneous Material.** Unless immediately destroyed, classified carbons, rejected copy, typewriter ribbons, ribbons from word processors, toner cartridges, printers, and the like shall be marked or labeled to indicate the level of classification and stored accordingly.

**2.30. For Official Use Only (FOUO).** Procedures for handling, marking, and processing information should be in accordance with references b and d.


Figure 1. Sample Standard Form 706, 707, 708, 709, 710, and 711

# CHAPTER 2
# CLASSIFICATION MANAGEMENT

## SECTION 3
## CLASSIFICATION PROHIBITIONS AND LIMITATIONS

### 2.31. Classification Prohibitions

a. Information will not be classified to:

(1) Conceal violations of law, inefficiency, or administrative error.
(2) Prevent embarrassment to a person, organization, or agency.
(3) Restrain competition.
(4) Prevent or delay the release of information that does not require protection in the interest of national security.

b. Basic scientific research information not clearly related to the national security may not be classified.

c. Information may not be reclassified after it has been declassified and released to the public under proper authority.

d. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under references e and f or the mandatory review provisions of section 3.6 of reference a only if such classification meets the requirements of reference a and is accomplished on a document-by-document basis with the personal participation or under the direction of the OIG, DoD, or the official designated under 5.6 of reference a. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under reference g.

e. Compilations of items of information, which are individually unclassified, may be classified if the compiled information reveals an additional association or relationship that:

(1) Meets the standards for classification under reference a and is not otherwise revealed in the individual item of information.
(2) As used in reference a, "compilation" means an aggregation of pre-existing unclassified items of information.

**2.32. Classification Challenges.** Reference a encourages individuals to challenge classification decisions as a means for promoting proper and thoughtful classification actions. As a result of this, OIG, DoD, procedures will ensure that no retribution or other negative actions are taken against any individual initiating such a challenge. Those authorized holders wishing to challenge the classification status of information should present such challenges to an OCA who has jurisdiction over the information. Such a formal challenge should be made in writing, but does not have to be specific other than to ask why the information is or is not classified, or is classified at a certain level.

**2.33. Classification Challenge Tracking System.** The OIG Security Division maintains a system for processing, tracking, and recording formal classification challenges made by authorized holders. The records of challenges will be subject to the attention of the Interagency Security Classification Appeals Panel (ISCAP), which is under the auspices of the ISOO. All classification challenges will be kept separate from Freedom of Information Act/Privacy Act requests with a separate record keeping system established to process and record the challenges.

**2.34. Classification Challenge Review Process.** Classification challenges will be reviewed by an OCA with jurisdiction over the challenged information. The OCA will provide a written response to the challenger within 30 days. If the challenger is not satisfied with the response, an impartial official or panel will review the challenger's request (supervisor of the OCA at the next highest level). If the challenge is not processed within 30 days, the OCA will acknowledge the challenge in writing and provide the challenger with a date when the OCA will respond. The acknowledgment must include a statement that if no response is received within 90 days, the challenger has the right to forward the challenge to the ISCAP for a decision.

**2.35. Reevaluation of Classification Because of Compromise.** The OIG Security Division, in conjunction with the Primary Office of Responsibility, shall prepare a written damage assessment and reevaluate information classified by the OIG, DoD, that has been lost or possibly compromised. The Office of Primary Responsibility shall promptly notify all holders of the information of any countermeasures taken to negate or minimize the effect of any compromise.

# CHAPTER 2
# CLASSIFICATION MANAGEMENT

## SECTION 4
## CLASSIFICATION GUIDES

**2.36. Classification Guides.** Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. Users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guides shall be reviewed as circumstances require, but at least once every 5 years. Each guide will be approved and in writing by an official who has program or supervisory responsibility over the information or is the senior agency official and is authorized to classify information originally at the highest level of classification prescribed in the guide. The OIG, DoD, will submit to the ISOO all declassification guides for final approval.

a. Classification guides shall, at a minimum:

(1) Identify the subject matter of the classification guide.

(2) Identify the original classification authority by name or personal identifier and position.

(3) Identify an agency point-of-contact with subject matter expertise.

(4) Provide the date of issuance or date of last review.

(5) State precisely the elements of information to be protected.

(6) State which classification level applies to each element of information and, when useful, specify the elements of information that are unclassified.

(7) State, when applicable, special handling caveats.

(8) Prescribe declassification instructions or the exemption category from automatic declassification for each element of information. When reviewing or updating a guide, the duration of classification prescribed for each element of information shall continue to correspond to the date of the guide's first issuance. When citing the exemption category listed in section 1.6(d)(8) of reference a, the guide shall also specify the applicable statute, treaty or international agreement.

(9) State a concise reason for classification, which, at a minimum, cites the applicable classification categories in section 1.5 of reference a.

b. Dissemination of Classification Guides. Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information. All classification guides will be submitted through the OIG Security Division for review and then forward to ISOO for final approval. The OIG Security Division will maintain a database of all classification guides approved and issued by the OIG, DoD. The OCA(s) will be responsible for obtaining approval of all classification guides before they are distributed.

# CHAPTER 2
# CLASSIFICATION MANAGEMENT

## SECTION 5
## DECLASSIFICATION AND DOWNGRADING

**2.37. Declassification and Downgrading.** Information will be declassified as soon as it no longer meets the standards for classification under reference a. It is presumed that information that continues to meet the classification requirements under reference a requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases, the information will be declassified. When such questions arise, they will be referred to the OIG Freedom of Information/ Privacy Acts (FOIA/PA) Office. The OIG FOIA/PA Office will determine, as an exercise of discretion, whether public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. Reference a does not amplify or modify the substantive criteria or procedures for classification; or create any substantive procedural right subject to judicial review. If the ISOO determines that information is classified in violation of reference a, that official may require the information to be declassified.

**2.38. Automatic Declassification.** Within 5 years from the date of reference a, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under reference g shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records will automatically be declassified no longer than 25 years from the date of its original classification, except for information that would:

a. Reveal the identity of a confidential human source, reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States.

b. Reveal information that would assist in the development or use of weapons of mass destruction.

c. Reveal information that would impair U.S. cryptologic systems or activities.

d. Reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system.

e. Reveal actual U.S. military war plans that remain in effect.

f. Reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States.

g. Reveal information that would clearly and demonstrably impair the current ability of U.S. Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized.

h. Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans.

i. Violate a statute, treaty or international agreement.

**2.39. Systematic Declassification.** Systematic declassification pertains to all classified agency records determined under Federal law to have permanent historical value wherever they may be stored. These records may be located or stored in:

a. The National Archives of the United States (including regional archive branches)

b. Federal Records Centers

c. Presidential Libraries

d. Agency file rooms or repositories

e. Other agencies

f. Other approved repositories, including contractor facilities, libraries, etc.

**2.40. Mandatory Declassification Review.** The OIG, DoD, will declassify information that no longer meets the standards for classification under reference a. A process has been established to provide a means to administratively appeal the denial of a mandatory review request and for notifying the requestor of the right to appeal a final agency decision to the ISCAP. Information requested under the FOIA/PA is released unless withholding is otherwise authorized or warranted under applicable law.

**2.41. Processing Requests and Reviews.** The OIG, DoD, may refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classified under reference a. When the OIG FOIA/PA Office receives any request for documents in its custody that contain information originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of reference a, the OIG FOIA/PA Office refers copies of requests and the pertinent documents to the originating agency for processing. After consultation with the originating agency, the OIG FOIA/PA Office may inform any requester of the referral unless such association is itself classified under reference a.

# CHAPTER 3
# SAFEGUARDING

## SECTION 1
## SAFEKEEPING AND STORAGE

**3.1. General Policy.** Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. Exceptions to these requirements should be approved by the OIG Security Division. The DoD policy concerning the use of force for the protection of classified information is specified in reference h. Weapons or sensitive items such as funds, jewels, precious metals, or drugs shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence Directives. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

**3.2. Standards for Storage Equipment.** The General Services Administration (GSA) establishes and publishes minimum standards, specifications and supply schedules for containers, vault doors, alarm systems and associated security devices suitable for the storage and protection of classified information. Reference i describes acquisition requirements for physical security equipment used within DoD.

**3.3. Storage of Classified Information.** Classified information is to be guarded or stored in a locked security container, vault, room, or area, as follows:

a. Top Secret information shall be stored in the following:

(1) A GSA-approved security container or modular vault, in a vault; or in the United States, in a secure room if under U.S. Government control. Other rooms that were approved for the storage of Top Secret in the United States may continue to be used. When located in areas not under U.S. Government control, the storage container, vault, or secure room must be protected by an intrusion detection system or guarded when unoccupied. U.S. Government control means access to the classified material is controlled by an appropriately cleared U.S. Government civilian, military, or contractor employee. An Intrusion Detection System (IDS) used for this purpose shall meet the requirements of reference b. Security forces shall respond to the alarmed location within 15 minutes from the time of notification.

(2) New purchase of combination locks for GSA-approved security containers, vault doors and secure rooms shall conform to Federal Specification FF-L-2740A. Existing mechanical combination locks will not be repaired. If the locks should fail, they will be replaced with locks meeting FF-L-2740A. These locks can be obtained through the Defense Supply Center in Philadelphia (DSCP) under National Stock Number 5340-01-469-5776.

(3) Storage requirements for Top Secret Compartmented Information are prescribed in other Director of Central Intelligence Directives.

b. Secret and Confidential. Secret and Confidential information shall be stored in the manner prescribed for Top Secret. It can be stored in an approved GSA security container or vault without supplemental controls or in secure rooms that were approved for the storage of Secret and Confidential material by the DoD components before October 1, 1995.

**3.4. Replacement of Combination Locks.** The mission and location of the activity, the classification level and sensitivity of the information and the overall security posture of the activity determines the priority for replacement of existing combination locks. All system components and supplemental security measures, including electronic security systems (e.g., automated entry control subsystems and video assessment subsystems), and level of operations must be evaluated by the OIG Security Division and coordinated with the Administration and Logistics Services Directorate, Office

of Administration and Information Management (OA&IM), when determining the priority for replacement of security equipment.

**3.5. Storage of Bulky Material**. Storage areas for bulky material containing classified information may have access openings secured by GSA-approved changeable combination padlocks (Federal Specification FF-P-110 series) or high security key-operated padlocks (Military Specification MIL-P-43607)

**3.6. Key Accountability**. The OIG components shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are used. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock. Reference j makes unauthorized possession of keys, key-blanks, key-ways, or locks adopted by any part of the DoD for use in the protection of conventional arms, ammunition or explosives, special weapons and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

**3.7. Procurement of New Storage Equipment.** New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule.

**3.8. Numbering and Designating Storage Facilities.** No external mark will reveal the level of classified information authorized to be or actually stored in a given container or vault. Priorities for emergency evacuation and destruction will not be marked or posted on the exterior of storage containers or vaults.

**3.9. Combinations to Containers and Vaults.** Combinations to security containers, vaults, and secure rooms shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

a. When placed in use.

b. Whenever an individual knowing the combination no longer requires access.

c. When the combination has been subject to possible compromise.

d. At least once every 2 years.

e. Once a year for safes containing NATO classified information.

f. When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

(1) Selecting Combinations. Combinations for each lock shall be unique to that lock and shall have no systematic relationship to other combinations used within a specific office. Combination numbers shall not be derived from numbers otherwise associated with the specific office or its personnel. The numbers within a combination shall be selected on a random basis without deliberate relationship to the other except to provide appropriate variance to operate the lock properly.

(2) Classifying Combinations. The combination of a container, vault, or secure room used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the classification. Declassification of combinations occurs at the time they are changed.

(3) Recording Storage Facility Data. A record shall be maintained for each vault or secure room door or container used for storage of classified information showing location of the door

or container, and the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. The SF 700, *Security Container Information*, shall be used for this purpose (see Figure 2, page 3-5).

(a) Part 1 of the SF 700. When completed, the form shall be placed in an interior location in security cabinets and on vault or secure room doors. To the extent practical, Part 1 shall be on the inside face of the locking drawer of file cabinets, and on the inside surface of map and plan cabinet and vault doors.

(b) SF 700, Parts 2 and 2A. Parts 2 and 2A shall be marked conspicuously on the front of the form with the highest level of classification and any special access notice applicable to the information authorized for storage in the container and will be stored in a security container other than the one in which they apply.

(c) Internal Security Containers. Internal security containers shall provide for prompt notification to the official responsible for the area if a container is found unsecured and unattended or shows evidence of unauthorized entry attempts or if the SF 700 is inaccessible or not available. Listings of persons having knowledge of the combination shall be continued as necessary on an attachment to Part 2. A minimum of two names will be entered on the form.

(d) Safe Combinations. Safe combinations will not be recorded on pieces of paper or other material with the following exception: persons having access to a number of combinations may, with the approval of their staff supervisor, record all combinations on an 8 1/2" x 11" page. This page will be classified and marked with the highest classification of material stored in the security containers and filed in a master security container. The combination to the container in which the page is stored will be memorized.

**3.10. Repair of Damaged Security Containers.** Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination as defined in reference k and are continuously escorted while so engaged. With the exception of frames bent through application of extraordinary stress, a GSA-approved security container manufactured before October 1990 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity as follows:

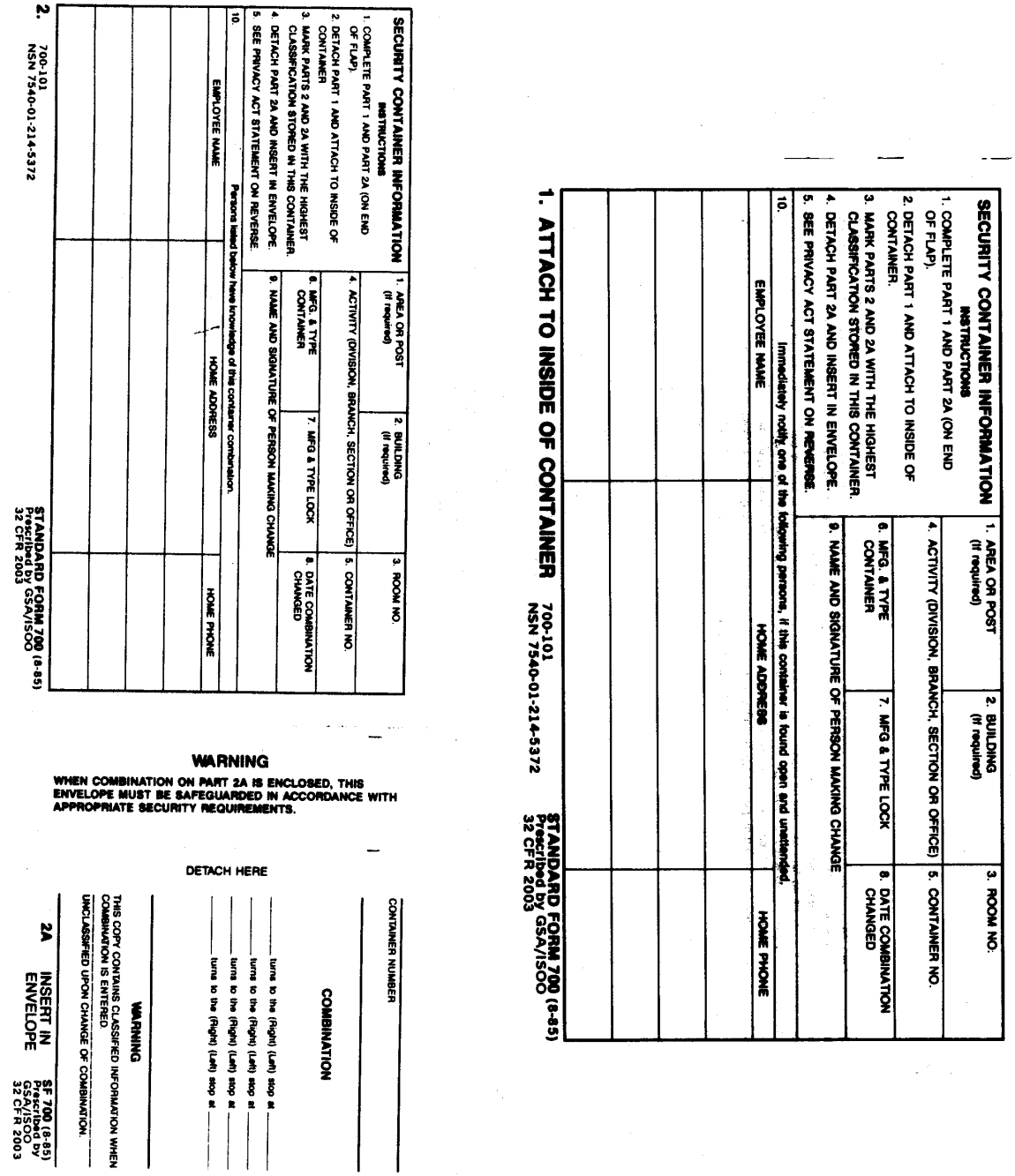
a. All damaged or altered parts, for example, the locking drawer, drawer head or lock, are replaced.

b. Has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, a replacement lock meeting FF-L-2470A is used, and the drilled hole is repaired with a tapered, hardened tool-steel pin, or a steel dowel, drill bit or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of rod a shallow recess not less than 1/8" nor more than 3/16" deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface.

c. Unapproved modification or repair of security containers and vault doors is considered a violation of the container or integrity of the door, and the GSA label shall be removed. Thereafter, they may not be used to protect classified information except as otherwise authorized in reference b.

**3.11. Moving/Turn-in of Safes**. Safes being moved to another location should be locked before moving and escorted by appropriately cleared personnel. Safes identified for turn-in will be inspected

by the cognizant Security Manager or personnel of the OIG Security Division to ensure no classified material remains therein. To prevent injury, OIG, DoD, personnel will ensure that all movement of safes is accomplished by the Administration and Logistics Services Directorate, OA&IM.



| SECURITY CONTAINER INFORMATION<br>INSTRUCTIONS | 1. AREA OR POST (If required) | 2. BUILDING (If required) | 3. ROOM NO. |
|---|---|---|---|
| 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). | 4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE) | | 5. CONTAINER NO. |
| 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. | 6. MFG. & TYPE CONTAINER | 7. MFG & TYPE LOCK | 8. DATE COMBINATION CHANGED |
| 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. | 9. NAME AND SIGNATURE OF PERSON MAKING CHANGE | | |
| 4. DETACH PART 2A AND INSERT IN ENVELOPE. | | | |
| 5. SEE PRIVACY ACT STATEMENT ON REVERSE. | | | |

**1. ATTACH TO INSIDE OF CONTAINER**

| 10. Immediately notify one of the following persons, if this container is found open and unattended. | | |
|---|---|---|
| EMPLOYEE NAME | HOME ADDRESS | HOME PHONE |
| | | |
| | | |
| | | |

700-101
NSN 7540-01-214-5372

**STANDARD FORM 700 (8-85)**
Prescribed by GSA/ISOO
32 CFR 2003

| SECURITY CONTAINER INFORMATION<br>INSTRUCTIONS | 1. AREA OR POST (If required) | 2. BUILDING (If required) | 3. ROOM NO. |
|---|---|---|---|
| 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). | 4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE) | | 5. CONTAINER NO. |
| 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER | 6. MFG. & TYPE CONTAINER | 7. MFG & TYPE LOCK | 8. DATE COMBINATION CHANGED |
| 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. | 9. NAME AND SIGNATURE OF PERSON MAKING CHANGE | | |
| 4. DETACH PART 2A AND INSERT IN ENVELOPE. | | | |
| 5 SEE PRIVACY ACT STATEMENT ON REVERSE. | | | |

10. Persons listed below have knowledge of this container combination.

| EMPLOYEE NAME | HOME ADDRESS | HOME PHONE |
|---|---|---|
| | | |
| | | |
| | | |

**2.**

700-101
NSN 7540-01-214-5372

**STANDARD FORM 700 (8-85)**
Prescribed by GSA/ISOO
32 CFR 2003

**WARNING**

**WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.**

DETACH HERE

CONTAINER NUMBER

**COMBINATION**

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

**WARNING**

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION.

**2A INSERT IN ENVELOPE**

**SF 700 (8-85)**
Prescribed by GSA/ISOO
32 CFR 2003

Figure 2, Sample Standard Form 700, Security Container Information

# CHAPTER 3
# SAFEGUARDING

## SECTION 2
## CUSTODIAL PRECAUTIONS

**3.12. Responsibilities of Custodians.** All OIG, DoD, employees are responsible for the safekeeping, handling, and storing of classified material in approved storage containers or facilities when it is not in use or under the supervision of an authorized person. Before releasing classified information to another individual, the holder of the material must ensure that person has the appropriate clearance and need to know for the information being released. The holder is defined as a person who has classified material in his or her possession, regardless of whether he or she has signed a receipt for the material. The OIG, DoD, employee who releases the information or discloses the information verbally to another individual must first ensure the individual is properly cleared and has the "need-to-know" for the information. *Security badges do not constitute security clearance level or need-to-know*. Verification of clearance will be made with the OIG Security Division.

**3.13. Residential Storage Arrangements.** The Chief, OIG Security Division, is the only approving authority to authorize removal of classified material from designated working areas in off-duty hours for work at home. The authorization will be based on whether the residence has an approved GSA security container.

**3.14. Care During Working Hours**. Classified material removed from storage shall be kept under constant surveillance by persons authorized access and having a need to know thereto and, when not in use, protected from unauthorized view of its classified contents until returned to storage. Such protection shall be provided, as applicable, by the material's unclassified cover or by an appropriate cover sheet. Cover sheets shall be Standard Forms 703, 704, and 705 for, respectively, Top Secret, Secret and Confidential documents (see Figure 3, page 3-11).

a. Cover sheets affixed to classified documents shall not be obscured by transmittal notes, routing sheets, etc.

b. Cover sheets will be removed from the document when the document is returned to the safe.

c. When documents are removed from classified storage files, a Charge Out Record, Optional Form 23 (or appropriate form), will be completed and will replace the document(s) when temporarily removed. When the documents are returned, the individual's name will be lined out and the form stored for future use (see Figure 4, page 3-12). Sign-out sheets, automated tracking systems and similar methods may be used.

d. Open containers including alarmed areas will be identified by a standard issue red "OPEN" sign displayed on the front of the container. Locked and checked containers will display the white reverse side of the sign "CLOSED." Containers with more than one built-in combination lock will have the "OPEN-CLOSED" sign displayed on each drawer having a combination lock.

e. The tops of security containers will be kept free of all material except the SF 702, Security Container Check Sheet (see Figure 5, page 3-13).

f. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, computer and typewriter ribbons, transfer medium, and other items containing classified information shall be safeguarded according to the level of classified information they contain and shall be accordingly destroyed after they have served their purpose. Transfer medium include drums,

cartridges, belts, sheets, memory, and other material in copiers, printers, facsimile, and other devices or items that receive or come in contact with classified information.

g. Destruction of personal computer printer or typewriter ribbons from which classified information can be obtained shall be accomplished in the manner prescribed for classified working papers of the same classification. After the upper and lower sections have been cycled through and overprinted five times in all ribbon or impact or typing positions, fabric ribbons may be treated as unclassified regardless of their previous classified use. Carbon and plastic ribbons and carbon paper that have been used in the production of classified information shall be destroyed in the manner prescribed for working papers of the same classification after initial use. However, any typewriter ribbon that uses technology that enables the ribbon to be struck several times in the same area before it moves to the next position may be treated as unclassified.

**3.15. End-of-Day Security Checks**. Each OIG component that processes, handles, and stores classified information will establish a system of security checks at the close of each working day to ensure that the area is secured. An SF 701, *Activity Security Checklist*, shall be used to record such checks. This form can be modified to suit the individual security (or safety) needs of the organization or particular office; i.e., entries for "STU-III CIK secured" or "coffee pot turned off." An SF 702, *Security Container Check Sheet*, shall be used to record the use of all vaults, secure rooms, and containers used for the storage of classified material (see Figures 5 and 6, pages 3-13 and 3-14).

a. **After Hours and Weekend Activity.** The SF 701 and the SF 702 shall be annotated to reflect after-hours, weekend, and holiday activity.

b. **Closing Containers.** An authorized person will record the date and time and initial the SF 702 in ink each time the container is opened or closed. When closing a container, the dial of the combination will be rotated at least four complete turns in the same direction and each drawer will be physically checked before the SF 702 is initialed.

c. **Checking Containers.** At the end of each workday, or when a security container is closed other than during normal duty hours, a person other than the one closing the container must check it, using the physical locking procedures described in the above paragraphs. The individual then will record the time checked and initial the form. This checking procedure will apply for each workday whether or not the security container was opened. The date and the statement "Not Opened" will precede the time and initials of the checker when the security container is not opened on a workday. A person other than the one locking the container must make the check of the container. Individuals working alone after duty hours may contact a nearby OIG, DoD, employee to check their container.

d. **Desk Check.** At the close of the workday, each occupant of a desk will thoroughly check each drawer to determine that it does not contain any classified material.

e. **Room Checks (Designated Security Checks).** Supervisors will designate a responsible individual for each workday to conduct a final security check of a working area using an SF 701. The security checker's designated area of responsibility may be a single room or a complex of rooms. The final security check will verify all classified material is properly secured.

f. **Personnel Working Late.** The minimum and normal procedure, when personnel are working late on a duty day, requires the designated security checker (usually the last person to leave an area) to conduct the final security check in all areas that have been secured and to complete the SF 701 for those areas. The security checker will then inform other personnel staying late that all areas are secured with the exception of the immediate area they are working in and that they are responsible for securing that area and completing the SF 701 when they finish their work.

**3.16. Emergency Planning.** Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities or enemy action. Such plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that the material does not come into the possession of unauthorized persons. Emergency plans shall provide for the protection of classified material in a manner that will minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement of authorized personnel around the affected area, pre-instructed and trained to prevent the removal of classified material by unauthorized personnel, is an acceptable means of protecting classified material and reducing casualty risk. Such plans shall provide for emergency destruction to preclude capture of classified material. (OIG, DoD, employees should refer to the OIG Emergency Plan and the OIG Continuity of Operations Plan (COOP) for detailed information.)

**3.17. Telecommunications Conversations.** Classified information shall not be discussed in telephone conversations except over approved secure communications circuits, that is, cryptographically protected circuits or protected distribution systems.

a. The Secure Telephone Unit-III (STU-III) and Secured Telephone Equipment (STE) is approved for classified discussions within the limitations displayed by the STU-III or STE. The need-to-know must be established before discussing classified information.

b. Users of secure telephones shall assure that only personnel with appropriate clearance and need-to-know are within hearing range of their conversation.

**3.18. Removal of Classified Storage and Information Processing Equipment.** Properly cleared personnel shall inspect classified storage containers and information processing equipment before removal from protected areas or unauthorized persons are allowed access to them. The inspection shall be accomplished to assure no classified information remains within the equipment. Some examples of equipment that shall be inspected are:

a. Reproduction or facsimile machines and other office equipment used to process classified information.

b. GSA-approved security containers, filing cabinets, or other storage containers used for safeguarding classified information.

c. Other items of equipment that may inadvertently contain classified information.

**3.19. Classified Discussions, Meetings, and Conferences**. The following procedures apply to hosting conferences, seminars or symposiums, exhibits, conventions, training courses, or other such gatherings during which classified information is disclosed, hereafter called a "meeting."

a. Before agreement to sponsorship, adequate security protective measures must exist or be provided far in advance of the meeting. The meetings will be held only at a U.S. Government installation or a U.S. contractor facility that holds an appropriate Defense Security Service Office Facility Security Clearance and where adequate physical and procedural controls have been approved.

b. Once an OIG component accepts sponsorship of a meeting, the component or its designated cleared contractor assumes overall security responsibility, ensuring that the invitations, etc., are unclassified; that all attendees have the appropriate level of clearances and the need-to-know has been certified; that access rosters are prepared, checked, and coordinated with the OIG Security Division; and that the subject matter, location, etc., of the meeting is coordinated with the appropriate Security Manager. Notification is given to the appropriate Security Manager if loss or compromise occurs before, during, or after the meeting. The OIG component also ensures that all participants are

advised of their security responsibilities; and that classified presentations are appropriately marked and safeguarded for later compilation and distribution through secure channels.

c. Classified information to be presented must be authorized for disclosure in advance by the U.S. Government department or agency having classified jurisdiction over the information involved. *Before showing or presenting the material, the briefer will announce the overall classification level of the slides being presented. Slides will not be shown unless the classification level is first disclosed by the presenter.*

d. If non-DoD members or foreign visitors are in attendance, OIG, DoD, contractors must obtain written approval from the OIG Security Division and Contracting Officer's Representative (COR) if they intend to disclose classified information.

e. Note-taking and electronic recordings shall not be permitted during classified presentations.

f. If foreign nationals are invited, a list of names, dates, and locations of the sessions they will attend will be forwarded to the appropriate local security office following the basic procedures of foreign disclosure policy. The OIG Security Division is responsible for:

(1) Providing guidance and assistance to sponsoring OIG components in developing and planning security measures for meetings.

(2) Monitoring meetings sponsored and conducted in the National Capital Region (NCR) by OIG components to ensure compliance with established security measures.

(3) Processing requests from OIG components concerning the attendance of foreign nationals at classified meetings and advising the requesting OIG component of approval or disapproval of the request.

**3.20. <u>Safeguarding U.S. Classified Information Located in Foreign Countries</u>.** Except for classified information that has been authorized for release to a foreign government or international organization and is under the security control of such government or organization, the retention of U.S. classified material in foreign countries may be authorized only when that material is necessary to satisfy specific U.S. Government requirements. This includes classified material temporarily transferred into a foreign country through U.S. Government personnel authorized to escort or hand carry such material. Whether permanently or temporarily retained, the classified materials shall be stored under U.S. Government control, as follows:

a. At a U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. At a U.S. Government activity located in a building used exclusively by U.S. Government tenants, if the building is under 24-hour control by U.S. Government personnel.

c. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host-government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

d. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants, but which is under host-government control, provided the classified material is stored in GSA-approved security containers that are further secured in locked room or area to which only U.S. personnel have access.

e. When the host government and U.S. personnel are collocated, U.S. classified material that has not been authorized for release to the host government shall be segregated from releasable classified material to facilitate physical control and prevent inadvertent compromise. U.S. classified material that is releasable to the host country need not be subject to the 24-hour U.S. control requirement provided the host government exercises its own control measures over the pertinent areas or containers during non-duty hours.

f. Foreign nationals shall be escorted while in areas where nonreleasable U.S. classified material is handled or stored. When required by operational necessity, foreign nationals may be permitted, during duty hours, unescorted entry to such areas provided the nonreleasable information is properly stored or is under the direct personal supervision and control of cleared U.S. personnel who can prevent unauthorized access.

g. Under field conditions during military operations, the commander may prescribe the measures deemed appropriate to protect classified material.

**3.21. <u>Non-COMSEC Classified Information Processing Equipment</u>.** The OIG, DoD, has a variety of non-COMSEC approved equipment to process classified information. This includes copiers, computers, facsimile machines, printers, scanners, cameras, electronic typewriters, and other word processing systems, among others. Because much of this equipment has known security vulnerabilities, its use can cause unauthorized disclosure. Such vulnerabilities will be reported to the OIG Security Division for handling.

a. Activities must identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Activity security procedures must prescribe safeguards to:

(1) Prevent unauthorized access to that information.

(2) Select equipment that performs the needed function and presents the lowest acceptable risk to the classified information the equipment processes.

(3) Comply with guidance on security vulnerabilities issued by appropriate authority and must report equipment problems and failures.

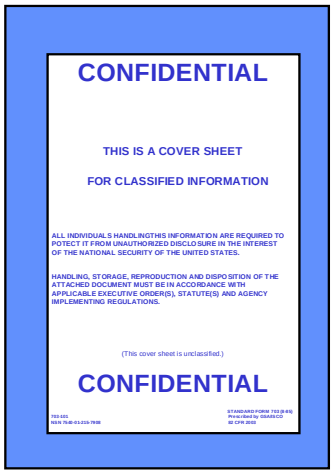
b. Reporting Equipment Problems and Vulnerabilities. The equipment that the OIG, DoD, uses to safeguard, destroy, or process classified information can fail to function properly or otherwise perform in a way that threatens that information. When that occurs, responsible individuals within the using activities must promptly:

(1) Restore the protection to the information.

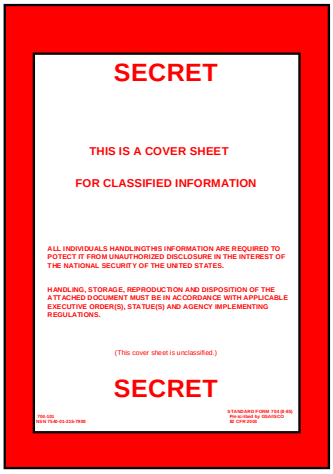
(2) Report the incident to the OIG Security Division. Such reports shall:

(a) Describe the problem, equipment type, manufacturer, serial number, the number of equipment units involved, and any means found to overcome the problem.

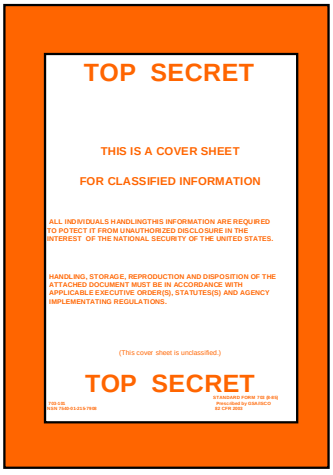
(b) Problems or vulnerabilities with COMSEC equipment and controlled cryptographic items shall be reported as prescribed by the controlling COMSEC authorities. The COMSEC authority shall promptly coordinate these reports and corrective actions, along with the Director, Counterintelligence and Security Programs, OASD (C3I), when the problems or vulnerabilities are common to all such equipment.




SF 705




SF 704




SF 703

Figure 3. Sample Classified Cover Sheets, SF 703, 704, and 705

# OUT

| **IDENTIFICATION OF RECORD (NUMBER, TITLE AND/OR SUBJECT, DATE OF FILE OR DOCUMENT** | **CHARGED TO** (PERSON & OFFICE) | DATE CHARGED OUT |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

OPTIONAL FORM 23
FEB 1962
GSA Circular No. 259

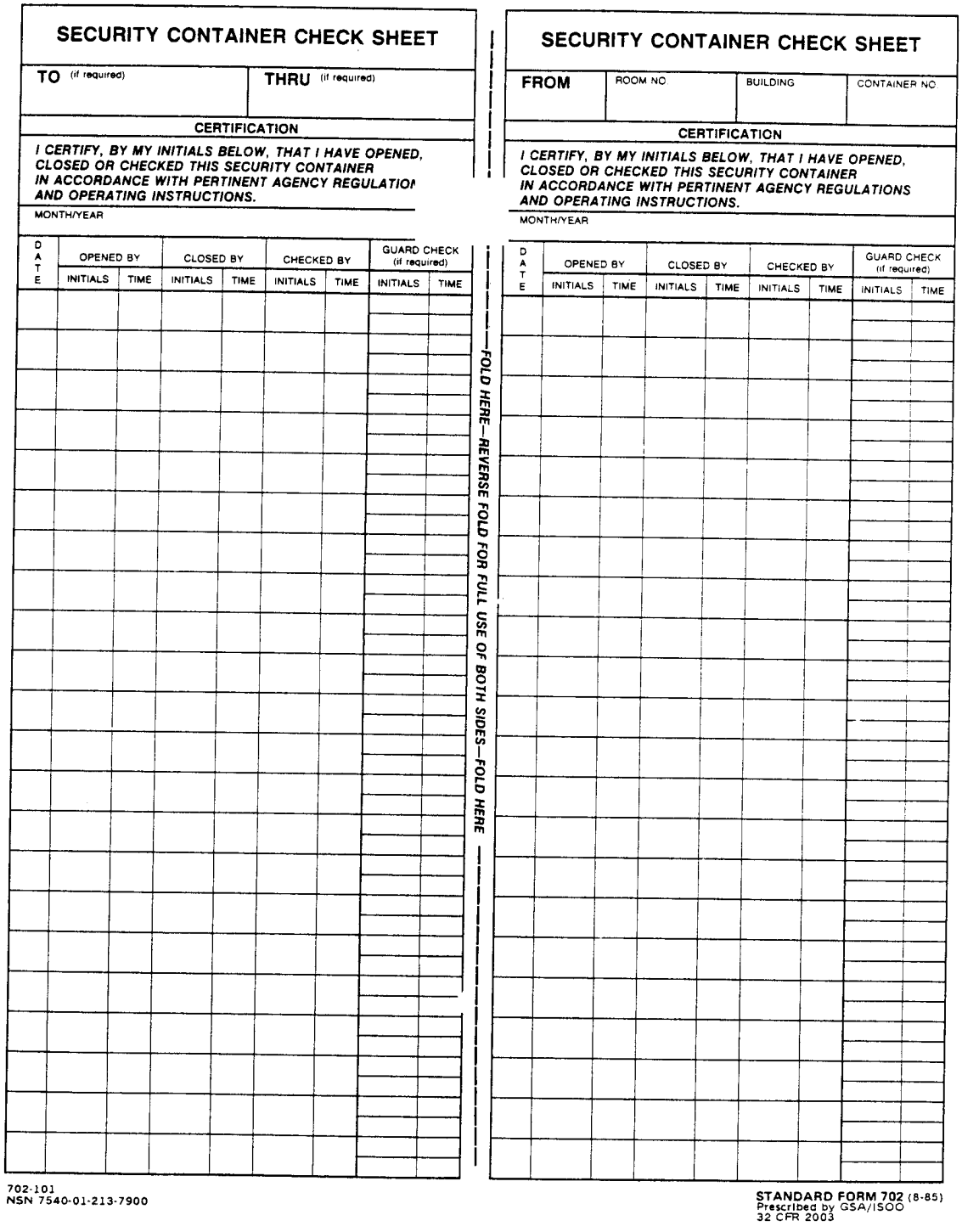
**CHARGOUT RECORD**
**5023-101**

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

DATE CHARGED OUT | (PERSON & OFFICE) **CHARGED TO** | **IDENTIFICATION OF RECORD (NUMBER, TITLE AND/OR SUBJECT, DATE OF FILE OR DOCUMENT**

OUT

Figure 4. Sample Optional Form 23, Charge Out Record



SECURITY CONTAINER CHECK SHEET

TO (if required) | THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIOI AND OPERATING INSTRUCTIONS.

MONTH/YEAR

| DATE | OPENED BY | | CLOSED BY | | CHECKED BY | | GUARD CHECK (if required) | |
|---|---|---|---|---|---|---|---|---|
| | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME |

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

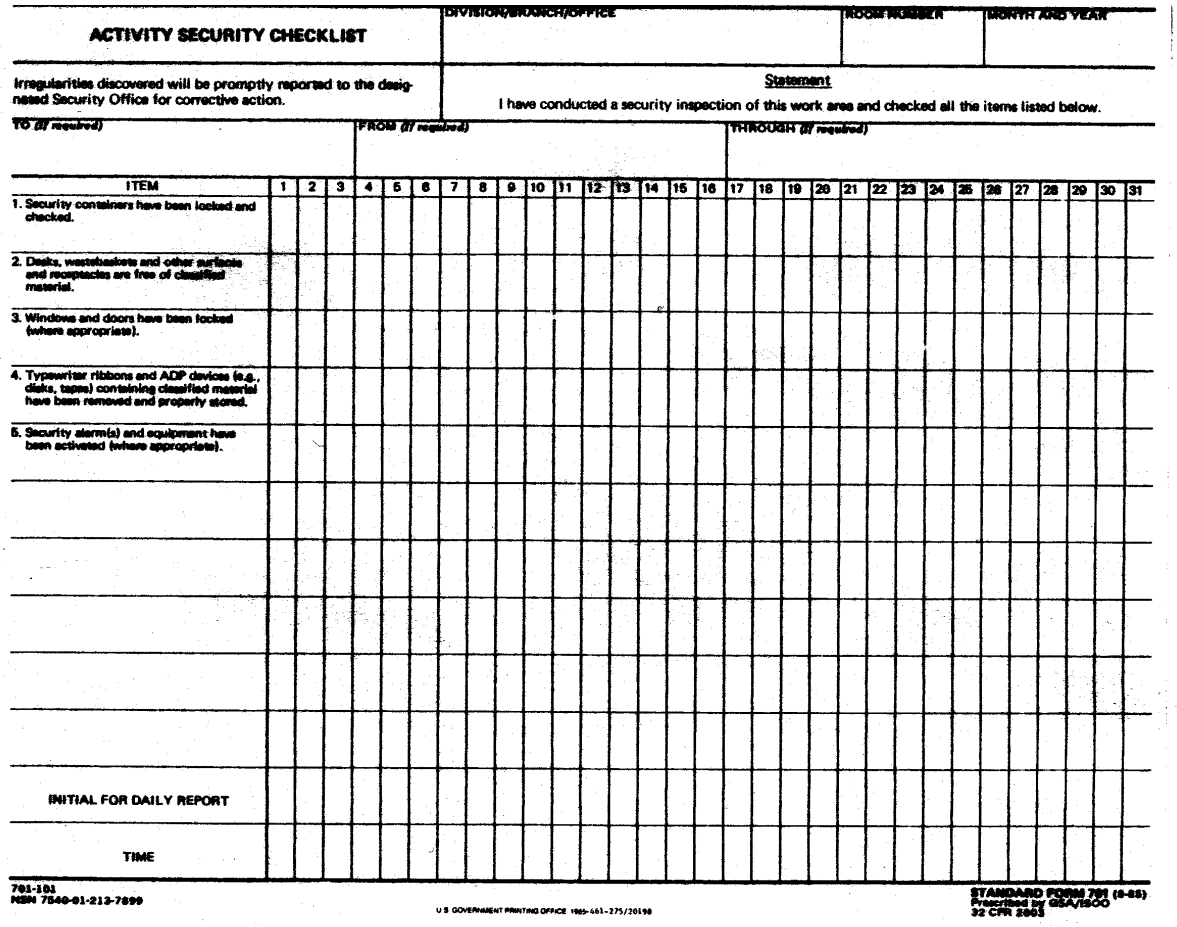
MONTH/YEAR

| DATE | OPENED BY | | CLOSED BY | | CHECKED BY | | GUARD CHECK (if required) | |
|---|---|---|---|---|---|---|---|---|
| | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME | INITIALS | TIME |

702-101
NSN 7540-01-213-7900

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 5. Sample Standard Form 702, Security Container Check Sheet



**ACTIVITY SECURITY CHECKLIST**

DIVISION/BRANCH/OFFICE | ROOM NUMBER | MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO (If required) | FROM (If required) | THROUGH (If required)

| ITEM | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. Security containers have been locked and checked. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Desks, wastebaskets and other surfaces and receptacles are free of classified material. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Windows and doors have been locked (where appropriate). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Security alarm(s) and equipment have been activated (where appropriate). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INITIAL FOR DAILY REPORT | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TIME | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

701-101
NSN 7540-01-213-7899

U S GOVERNMENT PRINTING OFFICE 1985-461-275/20198

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 6. Sample Standard Form 701, Activity Security Checklist

# CHAPTER 4
# CLASSIFIED DOCUMENT CONTROL

## SECTION 1
## ACCESS

### 4.1. General Restrictions on Access

a. A person may have access to classified information provided that:

(1) The Inspector General or his designee has made a favorable determination of eligibility for access.

(2) The person has signed an approved nondisclosure agreement.

(3) The person has a need-to-know for the information.

b. Classified information shall remain under the control of the originating agency or its successor in function. The OIG, DoD, shall not disclose information originally classified by another agency without its authorization. An official or employee leaving the OIG, DoD, may not remove classified information from OIG, DoD, control. Classified information may not be removed from any OIG, DoD, official premises without proper authorization.

### 4.2. Policy

a. SF 312, *Classified Information Nondisclosure Agreement (NDA)* (previously SF 189). Any person who requires access to classified information shall be required to sign a nondisclosure agreement as a condition of access. Currently, an SF 312 is the only form used to record newly executed agreements (see Figure7, page 4-5).

b. Briefings. At the time a OIG, DoD, member or employee is asked to sign an SF 312, the Security Manager or OIG Designated Personnel Representative will ensure that a briefing is provided that addresses the purpose of the NDA, the intent and scope of its provisions, the consequences that will result from the member's or employee's failure to sign the agreement, and the consequences that may result from the unauthorized disclosure of classified information, including possible administrative, civil or criminal sanctions. In addition to the NDA, personnel will sign and read aloud the Security Attestation Statement. The SF 312 and Attestation Statement will be maintained in the OIG Security Division file.

c. Implementation. Security Managers or Designated OIG Personnel Representatives will ensure the briefing and the request to sign the SF 312 occur immediately before the employee is granted access to classified information. The signed SF 312 will be forwarded to the OIG Security Division. The NDAs remains valid for a 50-year retention period. The OIG Security Division will retain previously signed copies of the SF 189 and SF 189-A, *Classified Information Nondisclosure Agreement* (the latter form applies only to cleared employees within industry) for 50 years. Any OIG, DoD, employee may, at his or her discretion, elect to substitute a signed SF 312 for a previously signed SF 189.

d. Access By Persons Outside the Executive Branch. Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

e. Consistent with law, directives, and regulations, the Inspector General or his or her designee shall establish uniform procedures to ensure that all AISs, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information has controls that:

(1) Prevent access by unauthorized persons.
(2) Ensure the integrity of the information.

f. Responsibilities:

(1) The OIG Security Division will serve as the OIG, DoD, focal point on all foreign disclosure matters.

(2) The OIG Component Heads and field activities will ensure that foreign visitors to their organizational elements are under escort at all times. The visitors will only receive classified information if authorized on an oral and visual basis only.

(3) All OIG, DoD, briefing officers will ensure that the information they provide to foreign visitors does not exceed that for which official approval has been granted.

(4) Limited Access Authorization. Requests for limited access authorization to classified information by foreign nationals, foreign governments and international organizations, under the provisions of reference b will be addressed to the OIG Security Division. Requests will include complete justification to support granting such access.

g. Visit Requests for Representatives of Foreign Governments. Requests by representatives of foreign governments visiting the OIG, DoD, or any OIG, DoD, field activity within the Continental United States (CONUS) must be processed through the Department of State and Defense Intelligence Agency (DIA). The request will then be forwarded to the OIG Security Division for appropriate action.

h. All OIG, DoD, personnel must be cognizant of the fact that:

(1) Classified information, released in an oral or visual manner, will relate only to the stated purpose of the visit and that no classified documents, tapes, recordings, or notes may be released unless such release has been approved.

(2) Classified minutes of any meetings attended by the foreign visitor will not be dispatched outside the OIG, DoD, until proper processing of the minutes has been accomplished and the OIG Security Division has obtained approval for release.

(3) Once a foreign visitor has been approved through the Department of State and DIA, no additions or deletions will be made without a complete restatement of the purpose.

i. Visitor Verification of Clearance and Safeguarding Capability. The OIG, DoD, policy requires that visitors shall provide advance notification of the pending visit in writing that establishes the visitor's security clearance and the purpose of the visit. An official other than the visitor who is in a position to verify the visitor's security clearance level shall sign requests. This is usually the visitor's security officer. Visit request letters will include the full name of the individual, date and place of birth, social security number, rank or grade of visitor, security clearance of the visitor, employing activity of the visitor, date and duration of the proposed visit, the purpose of the visit in sufficient detail, and the names of persons to be contacted. Visit requests will remain valid for not more than 1 year. The OIG Security Division, upon receipt of visitor certification letters, will consolidate all requests and provide the guard desk with an updated visitor certification roster. Visitors who appear on the list will be granted a "no escort required badge." The OIG Security Division will notify the office the person is visiting to provide confirmation of the level of access and safeguarding level of the visitor.

j. OIG, DoD, Visit Requests. The OIG Security Division will certify all requests for visits to other agencies and facilities requiring clearance verification. Requests will be submitted immediately after the visit is confirmed, but no later than 1 week before departure, to ensure processing and receipt by the visiting activity. The sample visit request (Figure 8, page 4-4) provides details for preparing the request.

k. Processing the Visit Request

(1) Submit an original plus two copies to the OIG Security Division. The original will be forwarded to the facility, the OIG Security Division will keep one copy on file, and one copy will be returned to the sender.

(2) One franked preaddressed envelope will be submitted with each request letter. Envelopes will be typed in all CAPS with no punctuation. If the letter is to be delivered to the Pentagon, an additional preaddressed (to Pentagon) messenger envelope, often referred to as "Holey Joe," must also be submitted.

(3) Print or type your name and office extension on a "Post-It" note and place it on the front of the packet. The appropriate person will be called when the letter is ready for pickup or if there is a problem with the request letter.

## CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

( Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

312-102

STANDARD FORM 312 (REV. 1-91)
Prescribed by GSA/ISOO
32 CFR 2003, E.O. 12356

Figure 7. Sample Standard Form 312, Classified Information Non-Disclosure Agreement

*(Prepare on OIG Letterhead)*

Office Symbol

(Facility/Activity Security Office) *(Include commercial telephone number and telefax number.)*

This is to certify the security clearance(s) of the following named individual(s) who will be visiting your facility: *(List personnel in alphabetical order by last name. The component security manager has the most current clearance information.)*

| **Visitor's Name, SSAN, DOB/POB, Citizenship** | **Type of Clearance Date Granted** | **OIG Component** |
|---|---|---|
| *DOE, John Edward<br>111-22-3333<br>11/29/51, Anywhere, OH, USA | SECRET<br>09/16/99 | OIR |
| *DOODY, Howdy NMI<br>222-333-4444<br>01/21/51, Tvland, CA, USA | Top Secret<br>10/11/00 | AUDIT |

*Indicates Team Leader or Project Manager

If the facility to be visited is located other than where the Security Office is located, you must indicate that below:

Point of Contact at the Facility: (Provide name, office and telephone number)

Period of Visit: 01 Jan 00 to 31 Dec 00 (Not to exceed 1 year)

Purpose of Visit: This security letter includes names of the individuals assigned to the subject audit. All individuals listed will not necessarily visit the activity at the same time. The period of the visit reflects the time of the anticipated audit work and report process.

OIG, DoD, Point of Contact and Telephone Number: *(Please do not list the OIG Security Division as the point of contact. Use a person who has knowledge of the visit and purpose of the visit.)*

John L. Henry
Chief, Security Division

**"PRIVACY ACT INFORMATION"**
**In compliance with the Privacy Act of 1974, this Information is Personal Data and must be protected from public disclosure.**

Figure 8. Sample Visit Request Letter

# CHAPTER 4
# CLASSIFIED DOCUMENT CONTROL

## SECTION 2
## DISSEMINATION

**4.3. Policy.** Except as provided by statute or directives issued pursuant to reference a, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. The Inspector General or his or her designee may waive this requirement for specific information originated within the OIG, DoD.

a. All OIG components and field activities shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know.

b. Each OIG component and field activity shall update, at least annually, the automatic, routine, or recurring distribution of classified information they distributed. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

### 4.4. Special Requirements for Release of Classified Intelligence Information to DoD Contractors

a. The following information will be provided to release classified intelligence information to a DoD contractor:

(1) Name and address of the contractor for whom the intelligence information is intended. (The security classification for which the contractor's facility is accredited [facility clearance and storage capability] is required for physical release of the information to the contractor's custody.) This information will be confirmed through the OIG Security Division.

(2) Contract number, date services began, and contract duration. If extensions of the contract or follow-on contracts are anticipated, so state.

(3) Name and address of the contracting activity.

(4) Name and telephone number of an OIG, DoD, point of contact for the contract.

(5) Complete identification of the intelligence information for which release approval is required. Identify issuing agency, document subject, security classification, and all restrictive control markings and statements. In addition, include a statement as to whether the material is locally available to the requesting agency.

b. Authorization to Release. The authorization to release will be based on the following criteria in that:

(1) Determination has been made that the specific intelligence document is necessary to enable the contractor to perform. (If only portions of intelligence documents will satisfy the requirement, only the intelligence that is actually required for contract performance will be considered for release.)

(2) National Intelligence Estimates, Special National Intelligence Estimates, National Intelligence Analytical Memorandums and Interagency Intelligence Memorandums are not released in their entirety to contractors. (Certain information contained therein may be released without identification as national intelligence.)

c. Special Requirements for Classified Intelligence. The Director, Central Intelligence Agency, has prescribed additional requirements and controls for classified intelligence in the

possession of contractors. The contracting authority must specifically include these requirements on the DD Form 254, *DoD Contract Security Classification Specification*. The contractor must:

(1) Maintain accountability for all classified intelligence information released to his or her custody, including confidential information.

(2) Obtain the written permission of the releasing authority before reproducing classified intelligence information. If permission is granted, each copy will be controlled in the same manner as the original.

(3) Obtain prior approval of the releasing authority before destroying classified intelligence, including Confidential.

(4) Restrict access to those individuals who possess the necessary security clearance and who are providing services under the contract. (Further dissemination to other contractors, subcontractors, other Government agencies, private individuals, or organizations are prohibited unless authorized in writing by the releasing authority.)

(5) Ensure that classified intelligence information is not released to foreign nationals or immigrant aliens, whether or not they are consultants, U.S. contractors or employees of the contractor and regardless of the level of their security clearance, except with prior permission from the releasing authority.

(6) Ensure that each employee having access to classified intelligence information is fully aware of the special security requirements for this material. The contractor will also maintain records in a manner that will provide, on demand, the names of individuals who have had access to this material.

(7) Return of Classified Intelligence Information. Upon termination of the contract, or earlier when the purpose of the release has been served, the contracting officer will require the contractor to return all classified intelligence information (furnished or generated) unless retention or destruction is authorized in writing by the releasing authority.

(8) Authority for Release. Requests for authority to release classified intelligence information originated by the intelligence community, as defined in reference l, will be submitted to the OIG Security Division. Each request must contain detailed justification for the release. Public release of Sensitive Compartmented Information (SCI) by contractors is not authorized.

# CHAPTER 4
# CLASSIFIED DOCUMENT CONTROL

## SECTION 3
## ACCOUNTABILITY AND CONTROL

**4.5. Collateral Top Secret Control Officer Program.** Top Secret information, if disclosed, could cause exceptional, grave damage to the security of the United States. A Top Secret Control Officer (TSCO) and at least one alternate will be appointed by each OIG component that prepares, receives, stores or handles Top Secret material. *Material received by OIG, DoD, offices must be logged in by the OIG TSCO and then receipted to the OIG component alternate TSCO for handling and safeguarding. All TSCOs and alternates must possess a final Top Secret clearance.* Except in unusual circumstances, the TSCO should not be the person designated as the OIG component's Security Manager. Top Secret material must be taken to the TSCO or alternate for processing into the Top Secret account. For field activities, the office manager will designate a TSCO and one alternate to accomplish matters affecting accountability and control of Top Secret material.

**4.6. Accountability.** A Top Secret Control Account (TSCA) is set up whenever Top Secret information is routinely originated, stored, received or dispatched. The TSCAs, to include central points for receipting and dispatching Top Secret Material, are limited to the minimum required for operational needs and functions of the office.

**4.7. Top Secret Registers.** The TSCO having accountability of Top Secret material will prepare an IG Form 5200-1-8, *Top Secret Register Page* (see Figure 9, page 4-11). Information received by or delivered to the Defense Courier Service (DEFCOS) will be taken to the Top Secret Custodian for accountability. The DEFCOS receipts suffice for accountability purposes in these cases. The TSCO attaches an IG Form 5200-1-5, *Top Secret Access Record and Cover Sheet* (or suitable form), to each Top Secret document (see Figure 10, page 4-12). When filled in, it will identify all persons given access to the information and the date of the disclosure. The person possessing the material ensures the recording is done; however, the name of the person granted access need only appear once regardless of the number of times the individual has had access to the information. Recording access is not required for personnel permanently assigned to a TSCA, computer center, computer tape library, telecommunications facility or printing and reproduction activity when duties involve processing large volumes of Top Secret material. This procedure is authorized only when entry to these areas is limited to assigned personnel identified on a roster. Such registers shall be retained for 5 years and shall, as a minimum, reflect the following:

a. Sufficient information to identify adequately the Top Secret document or material, to include the title or appropriate short title, date of the document, and identification of the originator.

b. The date the document was received.

c. Ensure each register page is assigned a consecutive number by including the calendar year and TSCA functional address symbol; for example, 99-IG-39. Alphabetical letters A, B, C, etc., are used when preparing continuation pages to the basic form. The register page number is also entered on the affected document to permit easier accomplishment of Top Secret inventories; however, care must be taken to not obliterate the permanently assigned originator control number.

d. Inactive Registers. This register reflects actions on documents no longer held in the office or agency. Documents that are transferred out of the office or agency, declassified or destroyed will be maintained for 5 years.

**4.8. Inventory.** The TSCO appointing authority, with action officers who use the information, annually review the volume and need for possessing the Top Secret material. The TSCO appointing

authority certifies this review when endorsing the inventory report. An inventory will be conducted on change of the TSCO. The frequency between any type of inventory may not exceed 12 months. The TSCO appointing authority will designate officials who understand Top Secret control procedures to conduct inventories. The number of inventory officials will be based on the scope and volume of Top Secret material. The TSCO or alternate of the account undergoing the inventory may not participate; however, a succeeding TSCO may be appointed. Inventory will determine if the TSCO is following proper procedures to ensure that that documents entered in the register are active and properly accounted for, and that all Top Secret material throughout the OIG, DoD, served by the account is properly entered in the register. The inventory team will do the following procedures:

a. Count register pages to verify completeness of the register.

b. View all documents in the register. Account for all Top Secret documents stored in OIG components and offices. Ensure each document has a receipt, or if the document was destroyed, a destruction certificate is on file.

c. Review the destruction process to verify correct procedures.

d. Review the inactive register, verify that documents listed are no longer the responsibility of the office being inspected; mark "audited" on the page, and have one team member initial and date the page. Entries so marked will not be re-inspected on subsequent inspections.

e. Attempt to resolve any discrepancies noted during the inventory, and treat as a possible security violation the inability to account for a document.

f. Submit a written report of the inventory to the OIG, DoD, Senior Information Officer (SIO), the OIG Security Division and forward one copy to the OIG, DoD, TSCO, who will retain the report for 5 years.

**4.9. Secret and Confidential Information.** Administrative procedures shall be established by each OIG component for receiving and dispatching Secret and Confidential information and material. The control system for Secret and Confidential information must be determined by a practical balance of security and operating efficiency and must meet the following minimum requirements:

a. Material received or dispatched outside any OIG component must show a record of receipt.

b. Records of receipts for Confidential and Secret material must be retained for a minimum of 2 years.

c. The OIG components shall develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained therein. Screening points shall be established to limit access to classified information to uncleared personnel.

**4.10. Working Papers.** Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

a. Dated when created.

b. Annotated with organization and office symbol of the originator.

c. Marked with the highest classification of any information contained therein.

d. Protected in accordance with the assigned classification.

e. Destroyed when no longer needed.

f. Marked in the manner prescribed for a finished document of the same classification when released by the originator outside the OIG component or transmitted electrically through message center channels.

**4.11. North Atlantic Treaty Organization (NATO) and Joint Chiefs of Staff (JCS) Documents.** Active accountability records must be maintained for NATO and JCS documents.

**4.12. Receipts.** Receipts are required for Secret and Confidential material sent outside the geographical confines of an OIG component or field activity.

**TOP SECRET REGISTER PAGE**
(DO NOT enter classified information on this form)

**I. DESCRIPTION OF DOCUMENT**

1. INDICATE: ORIGINATOR, TYPE OF INFORMATION (Letter, message, plan, vredo-tape, disk, etc.) DATE OF INFORMATION, UNCLASSIFIED SUBJECT TITLE, ORIGINATOR CONTROL NUMBER, COPY NUMBER(S), AND DATE RECEIVED. ALSO USE THESE DATA ELEMENTS FOR DESCRIBING ANY ATTACHMENTS THAT WOULD REQUIRE A RECEIPT IF TRANSMITTED SEPARATELY

**II. RECORD OF DOCUMENT CHANGES**

| 2. CHANGE NO.. | 3. COPY NO. | 4. DATE | 5. CLASSIFICATION | 6. ORIGINATOR | 7. ORIGINATOR CONTROL NO. | 8. COPY NO. OF BASIC DOCUMENT POSTED TO |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |

**III. DISPOSITION OF DOCUMENT**

**SECTION 1**

| 9.COPY NO. | 10. TO | 11. DATE | 12. TYPE OF ACTION | 13. SIGNATURE(S) | |
|---|---|---|---|---|---|
| | A. | A. | A. ACCOUNTABILITY TRANSFERRED | A. | |
| | B. | B. | B. ACTION, REVIEW, OR COORDINATION | B. | |
| | | C. | C. DOCUMENT RETURNED | C. | |
| | | D. | D. DOCUMENT DESTROYED OR | D. | |
| | | E. | E. COMMITTED TO CENTRAL DESTRUCTION FACILITY | E. | |
| | | F. | F. OTHER (Specify) | F. | |
| | | G. | G. AUDITED | G. | |

**SECTION 2**

| 9.COPY NO. | 10. TO | 11. DATE | 12. TYPE OF ACTION | 13. SIGNATURE(S) | |
|---|---|---|---|---|---|
| | A. | A. | A. ACCOUNTABILITY TRANSFERRED | A. | |
| | B. | B. | B. ACTION, REVIEW, OR COORDINATION | B. | |
| | | C. | C. DOCUMENT RETURNED | C. | |
| | | D. | D. DOCUMENT DESTROYED OR | D. | |
| | | E. | E. COMMITTED TO CENTRAL DESTRUCTION FACILITY | E. | |
| | | F. | F. OTHER (Specify) | F. | |
| | | G. | G. AUDITED | G. | |

| 14. REGISTER PAGE NO. | 15. RECONTROLLED TO REGISTER PAGE NO. | 16. RECONTROLLED TO REGISTER PAGE NO. |
|---|---|---|
| | | |

IG Form 5200.1-8, October 8, 1987

Figure 9. Sample IG Form 5200.1-8, Top Secret Register Page

# TOP SECRET ACCESS RECORD AND COVER SHEET

**The following personnel have been given access to or disclosure of information in the attached document on the date shown. DO NOT enter classified information on this form. Only record initial access to or disclosure of the information.**

| NAME AND GRADE | FUNCTIONAL ADDRESS SYMBOL | DATE |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| ORIGINATOR OF TOP SECRET DOCUMENT | ORIGINATOR CONTROL NUMBER | REMARKS |
|---|---|---|
| REGISTER PAGE NUMBER | DATE ACCOUNTABILITY TERMINATED | |

IG FORM 5200.1-5, October 1987

Figure 10. Sample IG Form 5200.1-5, Top Secret Access Record and Cover Sheet

# CHAPTER 4
# CLASSIFIED DOCUMENT CONTROL

## SECTION 4
## REPRODUCTION

**4.13. Restraint on Reproduction.** Requests for reproduction of Confidential, Secret and special category material will be used to document approval for reproduction and will be submitted on IG Form 5200.1.1, *Authorization for Reproduction of Classified Material*. Top Secret material can only be reproduced by the Top Secret Custodian. Alternate TSCO's must gain the approval of the TSCO before reproducing any Top Secret material (see Figure 11, page 4-15).

**4.14. Key Operators.** Key operators will be designated in writing by OIG components and field activities, for each copier that has been approved for reproduction of classified material. A copy of all appointment letters will be forward to the OIG Security Division. The key operator will ensure that reproduction of Top Secret and special category material has been authorized by the approving official and will monitor the copier while it is used for this purpose.

a. A key operator can be any responsible individual who can reasonably monitor the use of the copier.

b. The key operator must be cleared to the highest level of classification the copier has been approved to reproduce.

c. A current list of key operators for copiers approved for classified reproduction will be maintained by the OIG component's security manager or monitor. One copy of each appointment letter will be forward and maintained in the OIG Security Division.

d. The key operator will not be held responsible for any unauthorized reproduction of classified material performed by another individual. Key operators are obligated to report classified reproduction that has not been coordinated through them or their security manager.

**4.15. Designation of Copiers.** The OIG components and field activities, in coordination with the OIG Security Division, will designate copiers approved for reproduction of classified material. The OIG components and field activities where the copier is located will ensure that the equipment is under constant surveillance by personnel responsible for enforcing the rules against unauthorized use or that the equipment is protected by safeguards approved by the OIG Security Division.

**4.16. Facsimile Machine Controls.** Some facsimile (fax) machines can be connected to the telephone system through a secure interface, such as the STU-III. These interfaces, accomplished in accordance with guidance issued by the National Security Agency (NSA), may be used for the transmission of classified faxes. The following controls are established for use of secure fax machines to transmit classified information:

a. The sender of a classified fax is responsible for verifying that the intended recipient/addressee has the appropriate security clearance and need-to-know. Further, the sender must adhere to classification limitations displayed by the STU-III (or other equipment).

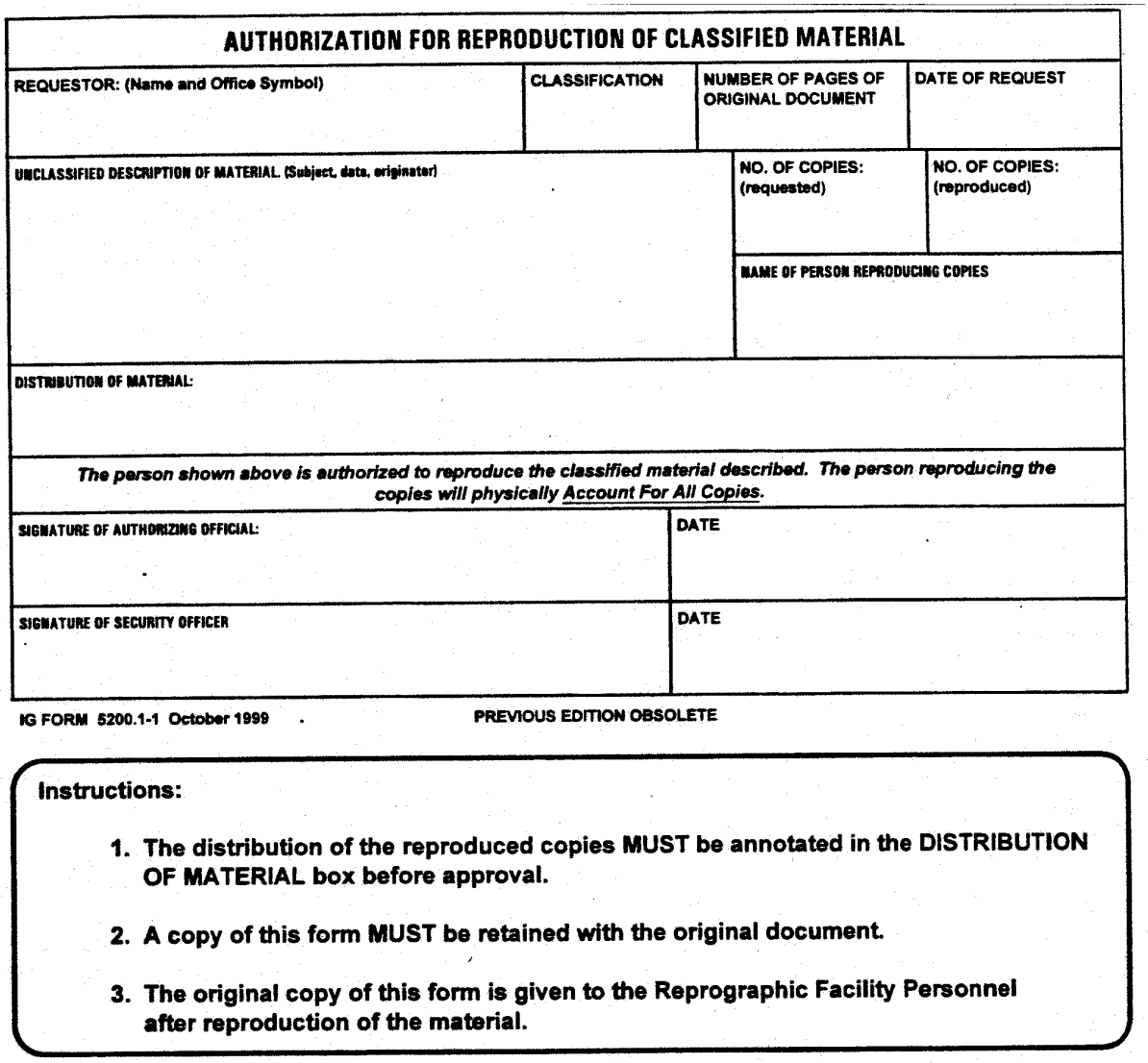
b. Transmission details shall be worked out before the actual transmission by the sender to ensure receipt of the classified fax by the intended recipient. In the case of transmitting Top Secret faxes, the sender must ensure that the intended recipient is personally available to receive the fax. All Top Secret faxes received will be taken to the TSCO for accountability.

c. Receipts for classified faxes shall be prepared by the sender and included with the transmission, executed by the recipient, and a signed copy faxed back to the sender.

d. The sender of a Top Secret fax is responsible for obtaining the consent of the originator of the Top Secret information to make the copy of the information that is inherent in the fax process.

e. Fax transmittal sheets will be used for all fax transmissions. An Unclassified Facsimile Header Page is used for the transmission of unclassified material; a Secure Facsimile Header Page is used for the transmission of classified material and serves as the receipt.

f. When receiving a secure fax, account for all pages. The user of the fax machine will ensure that no classified material is left in the fax machine and, that the STU-III Crypto Ignition Key (CIK) is returned to secure storage.



**AUTHORIZATION FOR REPRODUCTION OF CLASSIFIED MATERIAL**

| REQUESTOR: (Name and Office Symbol) | CLASSIFICATION | NUMBER OF PAGES OF ORIGINAL DOCUMENT | DATE OF REQUEST |
|---|---|---|---|
| | | | |

| UNCLASSIFIED DESCRIPTION OF MATERIAL. (Subject, date, originator) | NO. OF COPIES: (requested) | NO. OF COPIES: (reproduced) |
|---|---|---|
| | NAME OF PERSON REPRODUCING COPIES | |

DISTRIBUTION OF MATERIAL:

*The person shown above is authorized to reproduce the classified material described. The person reproducing the copies will physically Account For All Copies.*

| SIGNATURE OF AUTHORIZING OFFICIAL: | DATE |
|---|---|
| SIGNATURE OF SECURITY OFFICER | DATE |

IG FORM 5200.1-1 October 1999 PREVIOUS EDITION OBSOLETE

**Instructions:**

1. **The distribution of the reproduced copies MUST be annotated in the DISTRIBUTION OF MATERIAL box before approval.**
2. **A copy of this form MUST be retained with the original document.**
3. **The original copy of this form is given to the Reprographic Facility Personnel after reproduction of the material.**

Figure 11. Sample IG Form 5200.1-1, Authorization for Reproduction of Classified Material

# CHAPTER 5
# TRANSMISSION

## SECTION 1
## METHODS OF TRANSMISSION OR TRANSPORTATION

**5.1. Policy.** Classified information may be transmitted or transported only as specified in this chapter. "Designated," as used in this chapter, means having been issued a DD Form 2501, *Courier Authorization*. The procedures for completing the DD Form 2501 shall provide for accountability of the forms. The OIG Security Division will issue all DD Forms 2501 (see Figure 12, page 5-3).

**5.2. Top Secret Information.** The Armed Forces Courier Service is now the Defense Courier Service (DEFCOS). For more guidance on using DEFCOS, see reference m. The OIG Security Division is the point of contact for issuing the courier service card. Transmission of Top Secret information shall be effected only by:

a. The DEFCOS.

b. Authorized DoD Component Courier Service.

c. If appropriate, the Department of State Courier System must used when transmitting any level of classified material or within foreign countries where the material might be subject or possible customs inspections or other examinations. The material will be sent by an authorized means to the Chief, Diplomatic Mail and Pouch Branch, Department of State, Washington DC 20520. The outer cover will show the above address, and the inner cover will show the address of the specific recipient.

d. Cleared and Designated U.S. military personnel and Government civilian employees by surface transportation.

e. Cleared and Designated U.S. military personnel and Government civilian employees on scheduled commercial passenger aircraft on flights outside the United States, its territories and Canada.

f. Cleared and designated DoD contractor employees within and between the United States and its territories provided that the transmission has been authorized in writing by the appropriate contracting officer or his designated representative, and the designated employees have been briefed on their responsibilities as couriers and escorts for the protection for Top Secret material.

g. Cryptographic system authorized by the Director, NSA, or via a protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanation Security system.

**5.3. Secret and Confidential Information.** Secret and Confidential information may be transmitted by:

a. U.S. Postal Service Express (USPS) mail within and between the 50 States, the District of Columbia and the Commonwealth of Puerto Rico. USPS Express mail shall be used only when it is the most effective means to accomplish a mission within security, time, cost and accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the USPS Express Mail Label 11-B may not be executed under any circumstances. Secret USPS Express mail shipments shall be processed through mail distribution centers or delivered directly to a USPS facility or representative. The use of external (street side) Express mail collection boxes is prohibited.

b. GSA Contract Carrier. The GSA contract carrier(s) shall be used only when it is the most cost-effective way to meet program requirements, given time, security and accountability restraints. The GSA contract carrier(s) may be used for the transmission of Secret and Confidential material only within the Continental United States (CONUS). Secret material must meet GSA contract carrier standard size and weight limitations. Under no circumstances should this mail be left unattended.

c. USPS Registered Mail Within and Between the United States and its Territories. USPS registered through the Army, Navy or Air Force Postal Service activities outside the United States and its territories, provided that the information does not at any time pass out of U.S. control and does not pass through a foreign postal system or any foreign inspection.

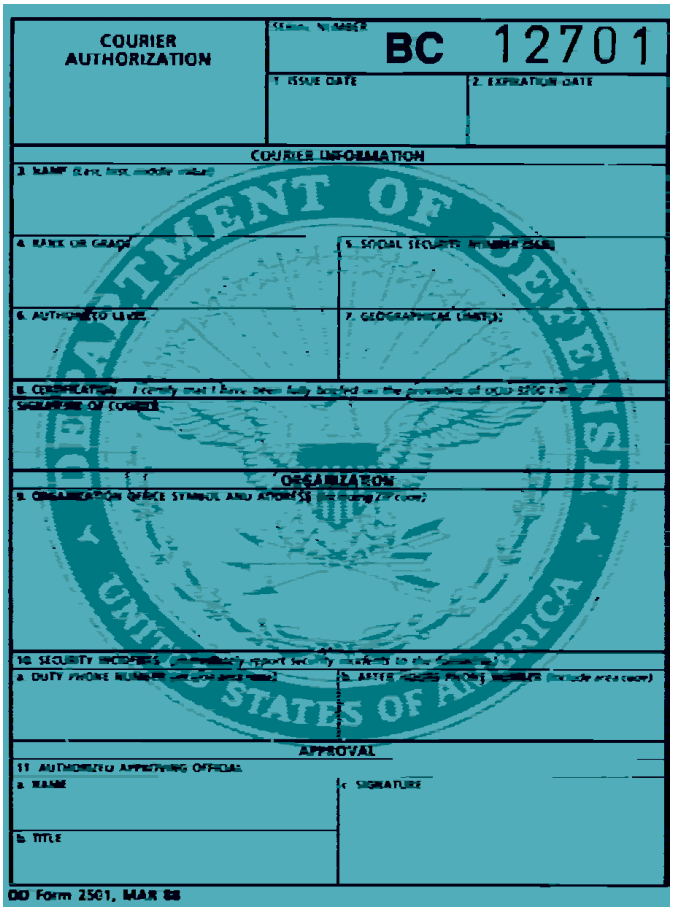
d. Carriers authorized to transport Secret information by way of a Protective Security Service (PSS) under the DoD Industrial Security Program. This is only authorized within U.S. boundaries. Routing for these shipments must be obtained from the Military Traffic Management Command (MTMC).

e. Cleared and designated DoD contractor employees within and between the United States and its territories provided that the transmission has been authorized in writing by the appropriate contracting officer or his designated representative, and the designated employees have been briefed on their responsibilities as couriers and escorts for the protection of Secret material.

f. Confidential information may be transmitted by means approved for the transmission of Secret information. USPS registered mail will be used for Confidential material to and from FPO and APO addresses located outside of the United States and its territories. USPS certified mail will be used for Confidential material addressed to DoD contractors or non-DoD agencies. USPS first class mail can also be used between DoD agency locations anywhere in the United States and its territories. If used, however, the outer wrapper must be marked “POSTMASTER: Return Service Requested. Do Not Forward.”

**5.4. Accountable Mail.** All custodians should ensure that accountable mail that is received as registered, certified from a GSA contract carrier (i.e., Federal Express), or unaccountable first class mail with the caveat "POSTMASTER: Address Correction Requested/Do Not Forward," is protected until its classification level is determined. All other first class mail, i.e., catalogs, vendor invoices and personal mail that, using prudent judgment, could not reasonably be expected to contain classified material is not required to be protected.

**5.5. Transmission of Classified Material to Foreign Governments.** To transmit classified material to a foreign government, obtain a signed receipt for all classified documentary information released. Show the complete unclassified title (or description of classified letter, minutes of meeting, etc.) and the numerical identification (when used) of documents being released on the form. Use USPS registered mail to transfer Secret or Confidential material to an embassy, official agency, or designated representative of the recipient foreign government when they are located within the United States.


COURIER AUTHORIZATION

BC 12701

1. ISSUE DATE

2. EXPIRATION DATE

COURIER INFORMATION

3. NAME (Last, first, middle initial)

4. RANK OR GRADE

5. SOCIAL SECURITY NUMBER (SSN)

6. AUTHORIZED TO LEVEL

7. GEOGRAPHICAL LIMITS

8. CERTIFICATION I certify that I have been fully briefed on the provisions of DOD 5200.1-R

SIGNATURE OF COURIER

ORGANIZATION

9. ORGANIZATION OFFICE SYMBOL AND ADDRESS (Including ZIP Code)

10. SECURITY INCIDENTS (Immediately report security incidents to the [illegible])

a. DUTY PHONE NUMBER (Include area code)

b. AFTER HOURS PHONE NUMBER (Include area code)

APPROVAL

11. AUTHORIZED APPROVING OFFICIAL

a. NAME

c. SIGNATURE

b. TITLE

DD Form 2501, MAR 88

Figure 12. Sample DD Form 2501, Courier Authorization

# CHAPTER 5
# TRANSMISSION

## SECTION 2
## PREPARATION OF MATERIAL FOR TRANSMISSION, SHIPMENT, OR CONVEYANCE

**5.6. Envelopes or Containers.** Under no circumstances will an SF 65, *U.S. Government Messenger Envelope* ("holey joe"), be used to transmit classified material. A GSA contract carrier envelope may be considered as the second envelope for purposes of double wrapping. When classified information is transmitted, it shall be enclosed in two opaque, sealed envelopes, wrappings or containers, durable enough to protect the material from accidental exposure or undetected deliberate compromise. Documents should be packaged so that classified text is not in direct contact with the inner envelope or container. When classified material is hand carried outside an activity, a locked briefcase may serve as the outer wrapper.

**5.7. Addressing.** Classified information shall be addressed to an official Government activity or DoD contractor with a facility clearance and not to an individual. This is not intended, however, to prevent use of office codes or such phrases in the address as "Attention: Research Department," or similar aids in expediting internal routing.

a. The attention line of the address on the outer envelope will appear as follows: "Attention: Security Office" (or "Officer") or "Document Control," as appropriate. When directing Secret or Confidential material to the attention of a particular member of an activity, the member's name may be indicated in an attention line on the inner envelope or container. The complete return address, including sender's office code, must be placed on the inner and outer envelopes or containers. The outer envelope or container shall not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

b. Classified material, under no circumstances, is to be mailed to the Senate or Congress. The Office of Congressional Liaison will hand carry packages for congressional delivery.

**5.8. Receipt System/SD Form 120.** See Figure 13, page 5-6.

a. An SD Form 120, *OSD Receipt for Classified Material*, will be used when transferring Top Secret, Secret, and Confidential information. The To, From, Classification, Date of Transfer, Description of Material Being Transferred, and number of copies blocks are mandatory items that must be filled out.

(1) If the material is being mailed, the following procedures will be followed:

(a) Separate the SD Form 120 before sealing the inner envelope.

(b) Keep the blue copy as the suspense for tracking the package.

(c) Attach the pink and yellow copies directly onto the material (report) inside of the inner envelope (it is highly advisable to place a return address label on the back of the yellow copy).

(d) Attach the white and green copies to the bottom left side of the outer envelope and record the receipt number on the envelope under the copies. The mailroom will sign and remove the copies, keeping the green and providing the white copy to the courier.

(2) When material is prepared for hand carrying to Congress, the following procedures will be followed:

(a) Keep the blue copy as the suspense for tracking the package.

(b) Attach the green, pink and yellow copies to the bottom left corner of the inner envelope (it is highly advisable to place a return address label on the back of the yellow copy.)

(c) Attach the white copy to the bottom left corner of the outer envelope. The Office of Congressional Liaison will sign and remove the white copy, providing it to the courier.

(3) When material is hand carried to locations other than the Congress, the following procedures will be followed:

(a) Keep the blue copy as the suspense for tracking the package.

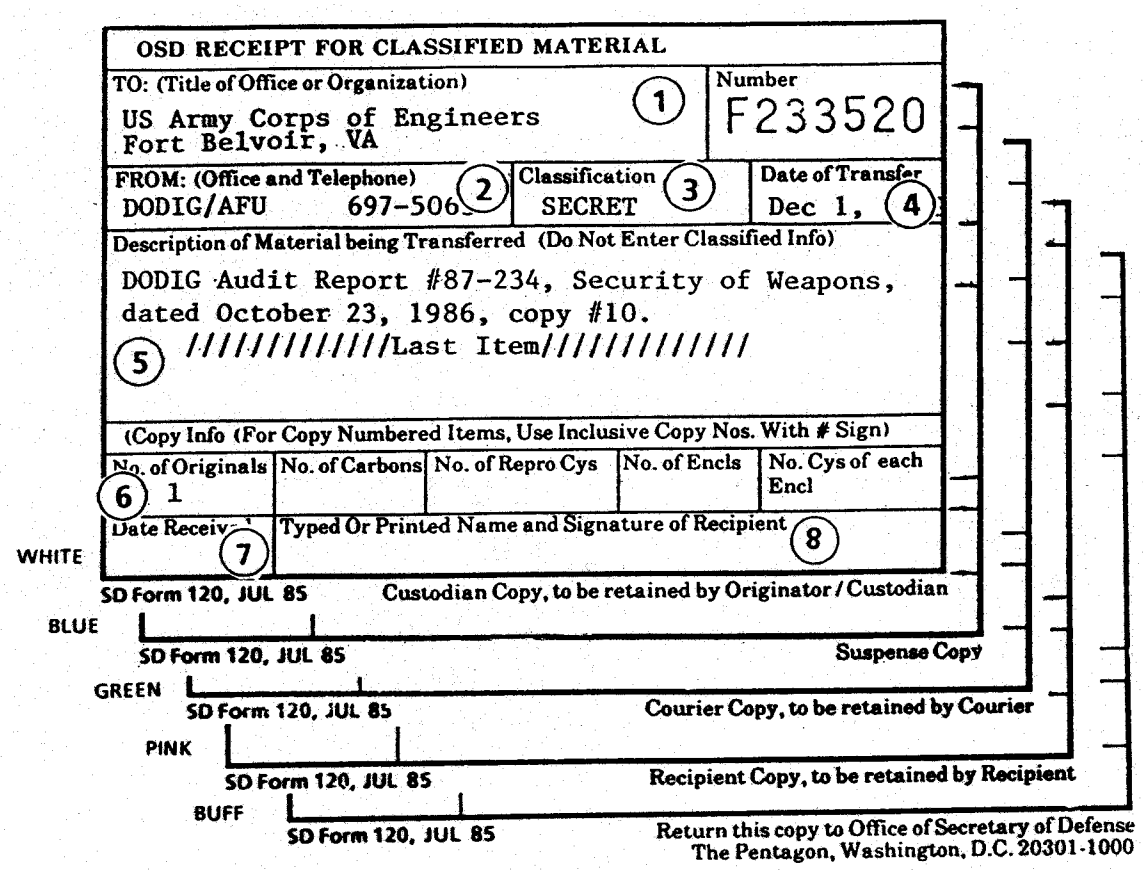
(b) Attach the remaining copies (white, green, pink and yellow) to the outer envelope. The recipient will retain the pink copy. The courier will return the signed white, green and yellow copies.

b. Receipts are also required for hand-to-hand transfer between OIG components that are geographically separated. When an OIG component receives a Secret document from outside the OIG, DoD, the recipient will sign and date the receipt and return it to the sender as soon as possible. When the document is no longer needed, a record of disposition will be kept for 2 years from the date of disposition (or destruction).

c. Receipt Forms. Any existing form may be used as a receipt for classified material if it adequately describes the material being transmitted. Developing new forms for this purpose is prohibited. Receipts will include the following information:

d. Tracer Actions. When a signed receipt is not returned within 30 days in CONUS or 45 days outside of CONUS, tracer action should be taken immediately. This applies to all classified material, including that being transmitted by DEFCOS. A copy of the receipt should be reproduced and marked "TRACER--ORIGINAL NOT RECEIVED." If the recipient did not receive the classified information, notify the OIG Security Division.

e. Classified Information Released to Contractors. An SD Form 120 will accompany all classified information released to contractors. The central office of record will maintain one copy, and another copy will be forwarded to the appropriate contracting office for inclusion in the contract file.




How to Prepare SD Form 120:

1. Functional address and location.
2. Functional address, location, and telephone number.
3. Classification level of classified documents.
4. Date the material is transmitted from the sending office.
5. Completely describe each classified attachment. When a subject or title is classified, use the unclassified short title. If the document is a message, use the identification elements.
6. Show the number of copies of each attachment and enclosure.
7. Date material received.
8. Self-explanatory.

Figure 13. Sample SD Form 120, OSD Receipt for Classified Material

# CHAPTER 5
# TRANSMISSION

## SECTION 3
## RESTRICTIONS, PROCEDURES, AND AUTHORIZATION CONCERNING ESCORT OR HAND-CARRYING OF CLASSIFIED INFORMATION

**5.9. General Restrictions.** The OIG, DoD, personnel are discouraged from hand carrying classified information on temporary duty (TDY), unless the information cannot be transmitted by other means. Hand carrying classified material is not authorized if other secure means of transmission are available. A DD Form 2501 is used to satisfy most policy requirements for written authorization to escort or hand carry classified material. The expiration date of the card will not exceed 2 years from the date of issue. Personnel will use an envelope, folder, or other closed container to prevent loss or observation of classified material hand carried outside of work areas. They should be provided with a written authorization when they are required to pass through an activity entry and exit inspection point to accomplish their classified information escort or hand carrying assignment.

**5.10. Approval Process.** The OIG, DoD, personnel required to act as couriers of classified material will submit a written Request for Approval to Escort or Hand Carry Classified Information Aboard Commercial Passenger Aircraft (see sample request at Figure 14, page 5-9) that must be approved by their respective, designated approving authority. DD Form 2501 will be issued only to those personnel whose duties require routine hand carrying of classified material. The OIG, DoD, personnel authorized infrequently to act as couriers for classified material will be designated by a courier authorization letter issued for each trip (see Figure 15, page 5-11). All couriers will receive an initial briefing and will be re-briefed annually on their responsibilities if the need for authorization remains valid. As a minimum, the courier briefing will include information on the following:

a. Espionage and terrorist threats.

b. Proper receipting and control procedures.

c. Physical protection, wrapping, and storage procedures.

d. Procedures to be taken in an emergency.

**5.11. Procedures for Hand Carrying Classified Information Aboard Commercial Passenger Aircraft.** The OIG, DoD, Component Heads, Program Managers, and Special Agents In Charge of OIG, DoD, field activities are designated approval authorities for authorizing personnel to hand carry classified information aboard commercial passenger aircraft, to include international flights. These officials will be referred to collectively as Designated Officials.

a. Local procedures established to justify TDY abroad shall require that the request for travel contain a written statement by the traveler that classified information will or will not (as applicable) be disclosed during the trip.

b. If the foreign disclosure of classified information is involved, an additional written statement will advise that disclosure authorization has been obtained in accordance with reference n. The statement also shall specify whether authorization has been obtained to carry classified material in compliance with reference b.

c. If the traveler has been authorized to carry classified material, a copy of the written authorization shall accompany the justification for the TDY. Block 16 of DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, shall contain the following statements:

(1) "Traveler is (or is not, as applicable) authorized to disclose classified information."

(2) "Traveler is (or is not, as applicable) authorized to carry classified material."

(3) "Traveler is aware of applicable export control, foreign disclosure, and security requirements."

(4) In addition to the above, the name and telephone number of the OIG Security Division will be entered in Item 16 of the DD Form 1610. The Chief, OIG Security Division, or Administrative Officer will apply his or her signature, thus indicating that the traveler has complied with the above requirements.

d. International Flights. Travelers who are authorized to carry classified material on international flights must have courier orders because DD Form 2501 is not valid for overseas travel. The traveler must be informed of and acknowledge his or her security responsibilities. This requirement, as a minimum, may be satisfied by a briefing or by requiring the traveler to read written instructions that contain the information listed below. The traveler will be held liable and responsible for the material described in the courier certificate. Throughout the journey, the classified consignment must stay in the personal possession of the traveler, except when it is in authorized storage. The classified material is not to be discussed or disclosed in any public place. The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities or embassies must be used. Classified material may not be stored in hotel safes. The traveler will not deviate from the authorized travel schedule. In cases of emergency, the traveler must take measures to protect the classified material. The traveler's security manager must provide appropriate guidance. The traveler is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents, etc.), are complete, valid, and current.

e. Dealing with Customs, Police, and Immigration Officials. There is no assurance of immunity from search by the customs, police and/or immigration officials of the various countries whose borders the traveler will cross. Should such officials inquire as to the contents of the consignment, the traveler will present the courier orders and ask to speak to the senior customs, police, and/or immigration official. This action should normally suffice to pass the material through unopened. If the senior customs, police, and/or immigration official demands to see the actual contents of the package, it may be opened in his or her presence, but should be done in an area out of sight of the general public. Precautions should be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other item. The traveler should ask the official to repack or assist in repackaging it immediately upon completion of the examination. The senior customs, police, and/or immigration official should be requested to provide evidence of the opening and inspection of the package by signing it when closed and by confirming on the shipping documents (if any) or courier certificate that the package has been opened. If the package has been opened under such circumstances as the foregoing, the addressee and the dispatching security manager will be informed in writing. Classified material to be carried by a traveler shall be inventoried, a copy of the inventory shall be retained by the traveler's security office, and the traveler shall carry a copy. The material shall be double wrapped, marked, and sealed as specified in reference b.

f. Travel Orders. Travel orders shall identify the traveler by name, title, and organization and include the traveler's passport or identification number. The orders shall describe the route to be taken by the traveler (the traveler's itinerary may be attached for this purpose); describe the package to be carried (size, weight and configuration); and contain the name, title, and telephone number of the responsible OIG component security manager who signed the orders. Upon completion of the trip, the traveler must return all classified material, appropriately packaged, or produce a signed receipt for any material that is not returned.

*(Prepare on OIG Letterhead)*

TO: (Approving Authority)

FROM: (Fill in)

THRU: (Chief, OIG Security Division)

DATE: (Fill in)

SUBJECT: Request for Approval to Escort or Hand Carry Classified Information Aboard Commercial Passenger Aircraft

Reference: DoD 5200.1-R, Information Security Program Regulation, January 1987

Preparer: (*Fill in*)

1. Request authority be granted to (*individual's name*) under the provisions of DoD Regulation 5200.1-R to hand carry classified documentation aboard a U.S. commercial passenger aircraft to (*country*). It is essential that the classified material in question be in (*country*) by (*date*).

2. The material is not present at the destination.

3. The material is needed urgently for (*a specified official purpose*).

4. Classification of information involved: (*fill in Confidential, Secret, or Top Secret*).

5. Description of the material: (e.g., three sealed packages, 9"x 8" x 24," addressee, and addressor).

6. Description of individual who will hand carry the information:

Name:
SSAN:
Rank/Grade:
Title:
Office Symbol:
Date of Birth:
Place of Birth:
Height:
Weight:

Figure 14. Sample Request for Approval to Escort or Hand Carry Classified Information Aboard Commercial Passenger Aircraft

7. Itinerary (all times local):

LV - date, time, carrier, flight #, airport
AR - date, time, carrier, country
LV - date, time, carrier, country, flight #, airport
AR - date, time, carrier, flight #, airport

8. Classified material to be hand carried will be in the physical control of the above named courier at all times. Storage of the classified material while in (*country*) will be at the facilities of (*U.S. Government installation or approved DoD contractor*) in (*city, country*).

9. Justification: (*Specify reason the material could not be transmitted by other approved means to the destination in sufficient time for the stated purpose*.)

*Signature of Requester*

Approved_____

Date_____

Figure 14 (Continued). Sample Request for Approval to Escort or Hand Carry Classified Information Aboard Commercial Passenger Aircraft

*(Prepare on OIG Letterhead)*

To: To Whom It May Concern
(Name of Airport)
(Location of Airport)

SUBJECT: Courier Authorization

1. This is to certify that the following named U.S. Government employee has been designated as an official courier:

Name: (Fill In)
Grade/Rank/Service: (Fill In)
SSAN: Fill In
DOB: (Fill In)
Height: (Fill In)
Weight: (Fill In)

2. Designated courier will present, upon request, the following identification: (*Military identification card or picture ID*).

3. The material to be hand carried by (*courier's name*) consists of (*description of package; e.g., one sealed envelope approximately 15" x 12" by 10"),* addressed to *(U.S. Government installation or DoD contractor facility*) and is to be opened only by appropriately cleared DoD personnel.

4. Request that you allow (*courier's name*) to personally hand carry and keep the material in (*his/her*) possession. It is further requested that such package not be subjected to baggage screening devices.

5. (*Courier's name*) will depart (*name of airport*) on (*departure date and time*) and arrive in (*city, state of destination*) on (*arrival date and time*).

6. This letter of authorization expires (*date*).

*To be Signed by the*
*Approving Official of TDY Orders*

Figure 15. Sample Courier Authorization Letter

## COURIER AUTHORIZATION BRIEFING

### 1. General

a. As a courier, you are responsible for protecting and safeguarding the classified defense information entrusted to you from unauthorized disclosure and compromise. While it is unlikely that you as a courier will be assaulted and the material in your possession removed by force, it is possible that you could find yourself in a hostage situation or confronted with a terrorist incident. In light of this danger, you must be aware of the action required to fulfill your responsibility as a courier of classified information.

b. Because of the danger of unauthorized disclosure, hand carrying of classified material is discouraged and should be resorted to only when time constraints preclude transmission through authorized channels.

### 2. Preparation

a. Before departure, you must submit to your Security Manager a list of all classified information to be hand carried, a copy of your itinerary, and approved storage arrangements en route and at your destination. Upon arrival, go directly to the approved storage facility to deliver or store the material.

b. You must be in possession of a DD Form 2501, *Courier Authorization Card,* or possess a courier letter authorizing you as a courier for the highest level of classified material to be transported. When traveling by commercial airlines within CONUS, U.S. territories and Canada, a courier authorization letter will be prepared and signed by the official signing your TDY orders. Block 16 of DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, shall contain the following statements for travel abroad:

"Traveler is authorized to disclose classified information."

"Traveler is authorized to carry classified material."

"Traveler is aware of applicable export control, foreign disclosure and security requirements."

(1) The name and telephone number of the security manager will be entered in Item 16 of the DD Form 1610; the security manager will apply his or her signature, thus indicating that the traveler has complied with the above requirements.

(2) If foreign disclosure of classified information is involved, there shall be an additional written statement that disclosure authorization has been obtained in accordance with reference n.

c. If traveling overseas, a memorandum to the appropriate approving authority through the OIG Security Division requesting a waiver from DoD regulations prohibiting hand carrying classified material aboard commercial must be prepared.

d. The material must be enclosed in two opaque wrappings in such a manner that the classified text does not directly contact the inner wrapping. The material used for wrapping must be of such strength and durability as to provide security protection while in transit, prevent items from breaking out of the container, and permit detection of all evidence of tampering. The wrapping must conceal all classified characteristics. When transported on commercial aircraft, each package will bear the signature of the official who signed the courier authorization.

(1) The outer label of the package will contain the correct address of an official U.S. Government activity or DoD contractor, with the proper facility clearance and safeguarding

capabilities, and your return address. The outer wrapping will not bear an individual's name, a classification, a listing of the contents divulging classified information, or any other unusual data or markings that might invite special attention to the fact that the contents are classified.

(2) The inner label of the package will also bear the correct address and return address but can designate an individual. The inner wrapping will be stamped with the highest classification level of classified material contained in the package; i.e., CONFIDENTIAL, SECRET or TOP SECRET. The inner wrapping will also be marked with special handling requirements. If the material is of a special nature, the statement, "TO BE OPENED ONLY BY_____" and the individual's name or title should be marked on the inner wrapping.

e. Classified information shall not be hand carried aboard commercial passenger aircraft unless there is neither time nor means available to move the information in the time required to accomplish objectives or contract requirements, including Requests for Quotation (RFQ) and/or Requests for Bid (RFB).

(1) When classified information is hand-carried across international borders, prior arrangements should be made by you as the requester to ensure the information will not be opened by customs, border, postal, or other inspectors, either U.S. or foreign.

(2) Ensure that the classified information carried contains no metal bindings and is contained in sealed envelopes.

(3) Ensure you have obtained the following documentation:

(a) An official ID card issued by a U.S. Government agency that carries photograph, descriptive data, and signature. (If the identification card does not contain date of birth, height, and weight, these items are included on the written authorization.)

(b) Original letters authorizing you to carry classified information. Reproduced copies are not acceptable. You must have a sufficient number of original signed letters to provide to each airline involved.

## 3. En Route

a. The classified package must be placed in approved storage (a hotel safe is not approved storage) at all stops en route to the destination, unless the information is retained in your possession and under your constant surveillance at all times. Hand carrying classified information on trips that involve an overnight stopover is not permissible unless you have made advance arrangements for proper overnight storage at a U.S. Government installation or a cleared contractor facility.

b. Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places. When traveling on a public conveyance, keep the package in hand or in contact with your body so that you will immediately be aware if it moves or is removed. If you leave your seat temporarily while in a public or private conveyance, you must carry the package with you. A locked car or its trunk, hotel or room, transportation terminal locker, etc., are not approved classified security containers.

c. When you transport classified material via private, public, or Government conveyance, you cannot store it in any detachable storage compartment, such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks.

## 4. Arrival

a. Upon arrival at your destination, you must go directly to the approved facility to deliver or store your material. If you deliver the material to someone, **be sure to get a signed package receipt**. It is your responsibility to verify that the recipient has the proper clearance and to notify him or her of the highest level of classified material in the package before releasing it. Whether departing or

returning to the Agency, **classified materials must not be stored at home.** If you return during non-duty hours with classified material, it must be stored in your office safe.

b. On TDY, if you must pass through customs upon your arrival, you usually will not be challenged if traveling with your official passport. If you are challenged, explain that you are an official U.S. courier, show the agent your courier authorization document and your orders, and point out the section that designates you as a courier. If this does not gain you entrance, ask to speak to the Senior Customs Official and repeat the above. If this fails, contact U.S. authorities for assistance (U.S. State Department officials). While telephoning for aid, **do not** leave your package in the hands of the Customs agents. Before resorting to calling local U.S. authorities, be sure of the exact requirements or wishes of the Customs agent's intended inspection. If he or she only wants to look at your package and it is properly wrapped, you may permit that. Under no circumstances will the official be allowed visual access to the actual classified material.

## 5. Terrorism

a. No person is immune to terrorism, and your position in a DoD agency makes you a possible target for espionage. Individual alertness, knowledge, and preparation for possible attempts are proven deterrents to such acts.

b. Everyone should be sensitive to possible surveillance. Avoiding predictable patterns and routines is one of the best individual means of protection against attacks.

c. If you suspect you are being followed, drive to the nearest safe location, such as a police station, fire station, or shopping center and ask for help.

d. When traveling overseas, do not travel in uniform if possible. Obtain any necessary foreign currency and/or traveler's checks before you leave, avoid corner "money changers" and displaying your currency. Do not transport weapons or facsimiles of them, alcohol, other than legally allowed beverages, narcotic substances (if needed for health reasons, take a prescription for each drug you must carry), prohibited books and publications, fireworks or other explosives, or aerosol tear gas even though it may be legal in certain areas. Restrict knowledge of your itinerary to office and family. If a change in your travel plans occurs, immediately notify your office and any office that might be expecting you.

e. If you encounter trouble: Remain calm and attempt to withdraw without being noticed. If you are in the United States, contact your security office. If you are abroad, contact the U.S. embassy or consulate (if no official U.S. representative is available, normally representatives from Australia, Canada, the United Kingdom or another friendly country will help you). Consult a consulate if you are a crime victim, if the authorities arrest you, or if you are injured or ill and hospitalized. Contact the local authorities if deemed necessary by the official consulate representatives. Finally, notify your local security office.

## CERTIFICATION

I certify that I have read and understand the requirements and responsibilities, to include those involving commercial aircraft travel, of a classified courier.

Date
_____

Signed
_____

Date Briefed
_____

Signature of Courier
_____

## COURIER PRE-DEPARTURE CHECKLIST

1. Do you have appropriate authorization? (Courier Authorization Letter or DD Form 2501, *Courier Authorization Card*?)

2. Is the Courier Authorization Letter (or DD Form 2501) dated?

3. Did you receive a courier briefing? If so, is there documentation to show this?

4. Does Block 16 of DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, contain the following statements (for TDY abroad)?

   a. Traveler is (or is not, as applicable) authorized to disclose classified information.

   b. Traveler is (or is not, as applicable) authorized to carry classified material.

   c. Traveler is aware of applicable export control, foreign disclosure, and security requirements. (This statement is to be used if either or both 4a and 4b above indicate that classified information is involved.)

   d. Has the Chief, OIG Security Division, or component security manager applied his or her signature to Block 16 of DD Form 1610, thus indicating that the traveler has complied with the above requirements?

   e. Have travel orders identified the traveler by name, title, and organization, and include the traveler's passport or identification number? Do they describe the route to be taken by the traveler? (The traveler's itinerary may be attached for this purpose.)

5. Does the inner envelope:

   a. Have a full destination and return address?

   b. Have appropriate classification markings and additional warning notices?

   c. Have sufficient wrapping to provide security protection, prevent contents from breaking out, and provide for the detection of tampering?

6. Does the outer envelope:

   a. Have a full destination and return address?

   b. Have a classification marking and additional warning notices? ***(This is prohibited, please correct immediately!)***

   c. Have sufficient wrapping to provide security protection, prevent contents from breaking out, and provide for the detection of tampering?

7. Have prior arrangements with a military installation or cleared contractor facility been made to allow for proper storage during overnight stops?

# CHAPTER 6
# DISPOSAL AND DESTRUCTION

**6.1. Policy.** Classified documents and other material shall be retained only if they are required for effective operation of the organization or if law or regulation requires their retention. Documents that are no longer required shall be destroyed or disposed of in accordance with the provisions of the Federal Records Act and other OIG, DoD, guidance. Destruction of classified documents shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

**6.2. Destruction of Material**. The OIG, DoD, has available two approved methods of destroying classified material. One is by shredding and the other is by burning.

a. **Shredders.** Approved crosscut shredders must be used to destroy classified information. When shredding controlled documents, an IG Form 5220.1-10, *Classified Material Destruction Certificate*, is required (see Figure 16, page 6-3). Signatures are required from two staff members (shredder and witness) when shredding Top Secret material and one signature is required when shredding Secret and Confidential material. Approved shredders have a crosscut of 1/2 x 1/32 or smaller.

b. **Burn Bags.** Classified material will be disposed of in red and white striped burn bags. Burn bags shall be marked to indicate the level of protection they require before destruction. Burn bags will also be marked with a name, office code, room number, telephone number and date. Burn bags are picked up at 400 Army Navy Drive on Mondays at 10 a.m. from the loading dock. Collection at Crystal Gateway North is on Tuesday at 9:30 a.m. from the loading dock. The IG Form 5200.1-26, *Burn Bag Receipt*, must be filled out and a copy provided to the person picking up the burn bags (see Figure 17, page 6-4). One copy of IG Form 5200.1-26 will be retained by the OIG component. The receipt is proof that the document has been burned and should be retained with classified document registers.

c. Destruction of For Official Use Only and Privacy Act Information. As defined by DoD guidance, For Official Use Only and Privacy Act information may be destroyed by "tearing each copy into pieces to preclude reconstruction or by shredding."

d. Other Material. Certain occasions may necessitate the destruction of classified or unclassified computer diskettes. This should be accomplished only when the diskette cannot be overwritten or if degaussing is impractical or unavailable. Computer diskettes should be disposed of in the following manner:

(1) Classified diskettes will be placed into burn bags marked "plastic." The number of diskettes, at any given time, must be kept to a minimum, and whole batches of diskettes must not be dumped into a burn bag. This is because the coating on the diskettes produces toxic fumes when burned and can present a health hazard to the personnel operating the incinerators in which burn bags are destroyed.

(2) Unclassified diskettes may be discarded with regular unclassified waste. That is, they may be placed into a regular office trashcan. The integrity of the diskette should be destroyed by cutting in half with scissors (for 5 1/4" diskettes) and bending in half or actually breaking (for 3 1/2" diskettes).

(3) Classified media will be disposed of and destroyed in accordance with the procedures described in the following paragraphs.

(a) Destruction of Hard Drives. Destruction of classified OIG, DoD, hard drives will occur at the NSA physical destruction office, Fort Meade, Maryland. Procedures for sending classified hard drives to NSA are available from the OIG Security Office.

. (b) Destruction of Expendable Media. Expendable media (e.g., magnetic tapes and diskettes) classified up to and including Top Secret will be placed in a burn bag and mixed with other classified waste. The burn bag will be disposed of with other classified waste. Plastic sleeves will not be placed in the burn bag, and the plastic disk will be removed and cut in half before placing in the bag.

(c) Destruction of SCI Media. Destruction of SCI media will occur in accordance with DIA policy. Contact the OIG Security Office for additional information on the destruction of SCI information.

(d) Destruction of SAP Media. Destruction of SAP media will occur in accordance with the SAP classification guidance. Contact the OSD-level SAP Central Office for additional guidance.

(e) Destruction of CD-ROMs. It is not required that unclassified CD-ROMs be "scratched" before they are sent to the destruction/recycling facility. The OIG components wishing to destroy Sensitive But Unclassified and FOUO CD-ROMs may still send them to the NSA CD-ROM destruction facility. Classified CD-ROMs will be destroyed using the NSA approved destruction method of controlled incineration, which meets environmental standards. The NSA accepts not only classified CD-ROMs, but also Sensitive But Unclassified and FOUO CD-ROMs. Procedures for mailing classified CD-ROMs to NSA are available from the OIG Security Office.

(f) Upon turn-in, hard disk drives will be overwritten and procedures will be implemented to verify the drives have been fully sanitized. If SCI was processed on the fixed hard drives the drives will be overwritten, sanitized, and removed for destruction.

(g) Destruction of Laser Printer Toner Cartridges. Laser printers use a replaceable toner cartridge with a platen (drum) that may retain classified images. Therefore, all laser printer toner cartridges used to process classified information are considered classified until sanitized or destroyed. These cartridges can be sent to the NSA Classified Material Conversion Facility for destruction.

**6.3. Annual Clean-Out Day.** The OIG, DoD, has designated December 6 (or the next work day if this date falls on a weekend) the date designated for an annual clean-out day. The number of cubic feet of classified material destroyed will be calculated and reported to the OIG Security Division for consolidation. (One cubic foot equals 2,500 pages; 1 safe drawer equals approximately 3 cubic feet or 7,500 pages.)

## CLASSIFIED MATERIAL DESTRUCTION CERTIFICATE

| TO: | FROM: (Office or Agency) |
|---|---|
| | |

| DESCRIPTION OF MATERIAL | DATE OF DOCUMENT | COPY NO. (If Any) | NUMBER OF COPIES |
|---|---|---|---|
| | | | |

| The material listed above has been (destroyed) (committed to the central destruction facility) according to IGDM 5200.1/DoD 5200.1-R. | DATE |
|---|---|

| Signature of Destruction/Commited to Destruction Official (Type or Print name) | Signature of Witnessing Official (Type or Print Name) |
|---|---|
| | |

IG Form 5200.1-10, October 1987

Figure 16. Sample IG Form 5200.1-10, Classified Material Destruction Certificate

DATE: _____

*MILITARY DEPARTMENT OR AGENCY:* ***INSPECTOR GENERAL, DoD***

OFFICE SYMBOL OR COMPONENT NAME: _____

TELEPHONE: _____

NUMBER OF UNCLASSIFIED BAGS: _____

NUMBER OF CONFIDENTIAL BAGS: _____

NUMBER OF SECRET BAGS: _____

NUMBER OF TOP SECRET BAGS: _____

BEGINNING SERIAL NO: _____

ENDING SERIAL NO: _____

NUMBER OF SCI BAGS: _____

TOTAL NUMBER OF BAGS: _____

NAME OF DELIVERY PERSON: _____

NAME OF DELIVERY PERSON: _____

NAME OF DELIVERY PERSON: _____

NAME OF DRIVER: _____

**DESTRUCTION PROCEDURES:**
For Headquarters, INSPECTOR GENERAL destruction is performed by the burning method. Burn bags are collected by the Pentagon Incinerator Plant personnel. For 400 Army Navy Drive, burn bag collection is each Monday between 11:45 a.m. and 12:00 noon at the loading ramp on the North side of the building. For 1111 Jeff Davis Highway, burn bag collection is each Tuesday 10:00 a.m. on the North side of the building.

**THE FOLLOWING PROCEDURES APPLY:**

1. Prepare a "Classified Material Destruction Certificate, IG Form 5200.1-10" listing the classified material being destroyed..
2. Inventory the classified material against prepared destruction certificates to ensure all material is accounted for.
3. Place the material identified for destruction in *RED STRIPED BAGS*.
4. Seal the bags/containers and mark them with the highest classification of information being destroyed.
5. Write on burn bag (s) the office symbol, telephone number and serial number of the bag.
6. Complete the Washington Headquarters Services (WHS) burn bag collection receipt. Have the bag pickup driver sign the receipt. Give the top copy of receipt to the driver and retain the second copy with the IG Form 5200.1-10.
7. Retain IG Form 5200.1-10 and bag collection receipts for 2 years. (5 years for Top Secret)

IG FORM 5200.1-26, OCTOBER 1994

Figure 17. Sample IG Form 5200.1-26, Burn Bag Receipt

# CHAPTER 7
# SECURITY EDUCATION

**7.1. Responsibility and Objectives.** All OIG components and field activities will ensure that the requirements of this chapter are implemented within their respective OIG components.

**7.2. Scope and Principles.** The scope of each security education program depends on the mission, functions of the activity and the degree of involvement with classified material.

**7.3. Security Education.** The effectiveness of the OIG, DoD, Personnel Security Program is proportional to the degree employees understand their responsibilities within the program. An integral part of the program is security education. To ensure that personnel become aware of their responsibilities, security education training is provided through the following briefings:

a. **Initial Briefings**

(1) Personnel granted a security clearance are not permitted access to classified information until they are briefed on the requirements of safeguarding classified information and sign a "Classified Information Nondisclosure Agreement (NDA)." The Personnel and Security Directorate,, OA&IM, will conduct the briefings for employees located within the NCR. The manager of OIG, DoD, field offices will ensure the briefings are conducted and documented. The completed NDA will be returned to the OIG Security Division for filing in the employee's Official Personnel Folder. Refusal to sign the agreement will result in access denial and clearance revocation.

(2) Supervisors will personally brief new employees on their individual security responsibilities. The briefing will be tailored to meet the employee's specific job requirements and must be accomplished within 30 days of assignment.

(3) A mandatory security indoctrination will be provided by the OIG Security Division for incoming personnel assigned within the NCR. For personnel located outside the NCR, the office manager will conduct the briefing.

b. **Refresher Briefings.** The OIG Security Division conducts annual refresher briefings for personnel in the NCR. The manager of OIG field offices will conduct the briefings for field personnel and forward certificates of completion to the OIG Security Division. This training reacquaints the employee with his/her responsibilities on the various requirements for handling classified information and other elements of the Personnel Security Program.

c. **Foreign Travel Briefings**. The OIG, DoD, personnel are required to report all foreign travel to the OIG Security Division. A foreign travel briefing may be required under certain circumstances. Foreign travel briefings are presented at the Pentagon on every Tuesday and Thursday at 12:00 noon in Room 1E801. Attendance is based on first come, first served. Attendees will receive a certificate upon completion of the briefing. A copy of the certificate must be given to the OIG Security Division to obtain credit for the briefing. A Foreign travel briefing is mandatory and required every 6 months.

d. **Termination Briefings**

(1) Military personnel and civilian employees receive a termination briefing when:

(a) Assignment and/or employment are terminated.

(b) A contemplated absence from duty or employment will last for 60 days or more.

(c) Access to classified and/or sensitive unclassified information is suspended.

(2) When any of those reasons apply, employees assigned within the NCR must report to the OIG Security Division to sign an IG Form 5200.2-1, *Security Termination Statement* (see Figure 18, page 7-3). The manager of OIG, DoD, field offices will ensure the briefings are conducted, documented and ensure that the completed form is returned to the OIG Security Division.

(3) If an employee refuses to execute a Security Termination Statement, an oral debriefing will be given in the presence of a witness and documented on IG Form 5200.2.1. The briefer and witness will sign beneath the statement attesting to the action, and the completed form will be forwarded to the OIG Security Division. The refusal to sign a Security Termination Statement will be recorded in the Defense Central Index of Investigations (DCII).

**DEPARTMENT OF DEFENSE**
**OFFICE OF THE INSPECTOR GENERAL**

## *SECUIRTY TERMINATION STATEMENT*

I am aware that my authorization for access to classified information with the Office of the Inspector General, DoD is hereby terminated in view of my pending termination of employment and/or assignment, administrative withdrawal of my security clearance, or any absence from duty for 60 days or more. I am aware of my continuing responsibility for safeguarding the fclassified information.
***I HEREBY CERTIFY THAT:***

1. I have read the provisions of the Espionage Act, Title 18, US Code, Section 793 and 794, and other criminal statutes and understand the implicataions thereof.

***I understand that one who unlawfully divulges information affecting the national defense is subject to severe criminal penalties and that the making of a false statement herein may be punished as a felony under Title 18, US Code, Section 1001.***

2. I have surrendered all material and documents containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency.

4. I shall report without delay to the Federal Bureau of Investigation, to an appropriate military authority, or the IG, DoD, Security Office, any attempt by any unauthorized person to solicit classified information.

5. I understand that my refusal to execute a Security Termination Statement will result in a verbal debriefing and such refusal will be reported to the Director, Defense Investigative Service for subsequent recording in the Defense Central Index of Investigations.

REFUSAL TO SIGN - ORAL DEBRIEFING

**"Oral briefing conducted:**
**Individual refused to sign."**

Debriefer Signature (Date)

Typed/Printed Name

Witness Signature (Date)

Typed/Printed Name

Signature (Date)

Typed/Printed Name

Debriefer Signature (Date)

Typed/Printed Name

IG Form 5200.2-1, October 1987

Figure 18. Sample IG Form 5200.2-1, Security Termination Statement

# CHAPTER 8
# COMPROMISE OF CLASSIFIED INFORMATION

**8.1. Policy.** To determine the circumstances of occurrence, a preliminary inquiry is immediately initiated into incidents of compromise, possible compromise, possible loss of classified information, or an infraction of the safeguarding controls as established by this Manual. A formal investigation will be conducted into complex incidents or those of serious consequence. At first, these incidents are referred to as information security incidents. In the course of the inquiry or investigation, the incident will be categorized as:

a. **Compromise**. The disclosure of classified information to persons not authorized access thereto.

b. **Possible Compromise**. A security incident in which a reasonable presumption exists that an unauthorized person had or has access to classified information.

c. **Inadvertent Access**. A security incident in which a person who is the subject of a favorable personnel security investigation had access to classified material for which he or she was not technically authorized to have or did not have a need to know.

d. **Security Deviation**. An incident that involves the misuse or improper handling of classified material but does not fall in the category of compromise, possible compromise or inadvertent access.

**8.2. Purpose of Inquiry or Investigation.** The purpose of an inquiry or investigation is to determine:

a. Whether or not a security incident has occurred.

b. The source and reason for the security incident.

c. Appropriate measures or actions to minimize or negate the adverse effect of the security incident.

d. The seriousness of damage to U.S. interests. (An OCA's damage assessment determines the seriousness of damage. Damage assessments are conducted when there is a reasonable expectation of damage to national security. The content of the inquiry or investigation report establishes a need, as applicable, for the OCA to conduct a damage assessment.)

e. Identify vulnerabilities in the security program that could result in similar incidents in the future.

**8.3. Debriefings in Cases of Unauthorized Access.** In cases where a person has had unauthorized access to classified information, it may be advisable to discuss the situation with the individual to enhance the probability that he or she will properly protect it. Whether such a discussion--commonly called a "debriefing"--is held will be decided by the OIG Component Head or responsible security officials. This decision must be based on the circumstances of the incident, what is known about the person or people involved, and the nature of the classified information. The following guidelines apply:

a. If the unauthorized access was by a person with the appropriate security clearance, but no need-to-know, a debriefing is usually unnecessary. A debriefing may be required if the individual is not aware that the information is classified and needs protection.

b. If the unauthorized access was by a Government employee or military member without the appropriate security clearance, a debriefing is appropriate. The person should be advised of his or her responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if he or she fails to do so. The debriefing official should make sure the individual understands what classified information is, why its protection is important and that the employee knows what to do should someone try to obtain the information. If the person who had unauthorized access is an employee of a contractor participating in the National Industrial Security Program, the same guidelines apply as for Government employees.

**8.4. Responsibility of Discoverer**. If classified information appears in the public media, OIG, DoD, personnel are cautioned not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. If approached by a representative of the media who wishes to discuss information believed to be classified, individuals should neither confirm nor deny the accuracy of the information and should report the situation immediately to the appropriate security and public affairs authorities.

**8.5. Appointment of Preliminary Inquiry Officer (PIO).** Upon notification of a security incident, the OIG Security Division will coordinate with the OIG Component Heads in appointing a PIO in writing. The OIG Security Division will be provided the name, office code, and telephone number of the PIO within 5 working days from the date of the requesting memorandum. The following individuals will take action after a security incident is reported:

a. The **Appointing Official** will:

(1) Appoint a PIO to conduct an expeditious, thorough inquiry or investigation whenever a security incident occurs. (The person appointed to conduct the inquiry must have an appropriate security clearance, must have the ability and available resources to conduct an effective inquiry and must not have been involved--directly or indirectly--in the incident. Except in unusual circumstances, the activity Security Manager should not be appointed to conduct the inquiry.) Approve/disapprove extensions if the PIO cannot meet the set suspense date and provide a courtesy copy of the extension approval to the OIG Security Division.

(2) Ensure any proposed disciplinary action is coordinated with the Personnel and Security Directorate, OA&IM, to determine whether the individual involved in the incident has any record of previous security violations. Any disciplinary action proposed against civilian employees is referred to the Employee Relations Division. Proposed disciplinary action against military members must be coordinated with the Director, Personnel and Security Directorate, OA&IM, and will comply with the provisions of the Uniform Code of Military Justice.

b. The **PIO** will:

(1) Obtain a briefing from the Security Manager to receive initial facts and evidence surrounding the incident.

(2) Consult with the OIG Security Division for technical guidance in conducting the inquiry.

(3) Prepare and forward, within 15 working days, a report that will include, as a minimum, the following sections:

(a) Authority. State when, where and by whom the inquiry was conducted.

(b) Classification of Material. What specific classified information and/or material was involved? What level of classification was it?

(c) Personnel Interviewed. List all personnel who were interviewed. Include their rank or grade, full name, duty title or functional address, and security clearance level.

(d) Facts. When, where, and under what circumstances did the incident occur? Exactly what happened? (Arrange in chronological order.)

(e) Conclusions

1 Brief summary of conclusions reached after a review of all pertinent information. Conclusions must be supported by the facts, and the evidence obtained during the inquiry process must support the facts.

2 What was (were) the cause(s)? What persons, situations or conditions caused or contributed to the incident?

3 Possibility of Compromise. Did compromise of classified information occur? If so, can damage to national security be expected? Every inquiry into compromise or possible compromise of classified information must include a judgment about whether compromise occurred and about the potential damage to national security. One of the following alternatives must be chosen:

a Compromise of classified information did not occur.

b Compromise of classified information may have occurred.

c Compromise of classified information did occur, but there is no reasonable possibility of damage to the national security.

d Compromise of classified information did occur and damage to national security may result.

4 Recommendation. Suggested corrective action to prevent future incidents.

**8.6. Handling Instructions.** The PIO will mark each page "FOR OFFICIAL USE ONLY" unless the report contains classified material, then mark accordingly. Route the report through the OIG Security Division for a technical review and further processing.

# CHAPTER 9
# INFORMATION SYSTEMS

**9.1. Background.** Information system(s) (IS) security is a multifaceted discipline. Protecting information being processed, transmitted, and/or stored by IS requires software and hardware security features, in addition to more traditional security disciplines, such as physical security and personnel security. IS security ensures the confidentiality, integrity, and availability of the information within the IS. IS is often referred to as Automated Information Systems (AIS) and Information Technology (IT). General security procedures applicable to the accountability, control, dissemination, reproduction, and destruction of national security and unclassified but sensitive information are provided in this chapter.

**9.2. General Requirements.** Within the OIG, DoD, the Chief Information Officer (CIO) is responsible for the direction, administration, and implementation of IS networks that process, store, reproduce, transmit, or otherwise handle classified or unclassified but sensitive information. When national security or unclassified but sensitive information is processed in an IS, the system will be accredited by a Designated Approving Authority (DAA).

**9.3. Certification and Accreditation Overview.** Agency officials are required to certify systems that meet all applicable Federal policies, regulations, and standards, and the results of system tests demonstrate that the Certification and Accreditation (C&A) process is proportional to the system size, mission criticality, data sensitivity, and security requirements. The scope of certification activities should depend on whether the system incorporates previously evaluated products or subsystems used in a system that has already been certified and accredited at the same level. The effort should be able to make use of C&A work done by other organizations. A complete system certification must consider factors dealing with the system in its unique environment, such as its proposed security mode of operation, clearance of user, applications, data sensitivity, system configuration, site/facility location, and connectivity to other systems. Personnel who are technically competent to assess the system's ability to meet the security requirements using an acceptable methodology should complete certification. The resulting documentation of the certification activities is provided to the DAA to support certification, such as risk analysis, security test and evaluation, and various types of evaluations.

**9.4. Overview of Modes of Operation.** Modes of operation are authorized variations in the operating environment of an IS. The type of information, clearance, and access level of users will determine the mode of operation. Systems are approved in one of four modes: dedicated, system high, multilevel, and multilevel partitioned. Authority to operate in one mode of operation precludes operation of the IS in a more restrictive mode without re-accreditation. The accreditation process and the requirements for each security mode are described in reference o.

a. **Dedicated Mode**. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the IS. If the IS processes special access information, all users require formal access approval. In the dedicated mode, an IS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

b. **System High Mode**. A mode of operation wherein all users having access to the IS must possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the IS. If the IS processes special access information, all users must have formal access approval.

c. **Multilevel Mode**. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all the data handled by the IS.

d. **Multilevel, Partitioned Mode**. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the IS.

## 9.5. Additional Security Concerns

a. **System Security Features**. System security features alone are inadequate to ensure secure operation of an IS. Additional controls must be established and implemented to ensure confidentiality, integrity and availability of hardware, software, and data.

b. **Encryption**. Encryption should be used when transmitting national security information on external devices. NSA-approved devices and key management systems will be used for recovery of plain text for a minimum of 5 years from the time of the encryption.

## 9.6. Physical Security

a. Physical security of systems processing national security information must be established and continuously maintained. The level of controls shall be commensurate with the highest classification level of the information handled by the IS and the environment in which the IS operates. Protective measures must prevent or detect unauthorized access through system entry points and unauthorized modification of computer hardware. Mission critical systems must have adequate security controls to prevent and/or detect unauthorized attempts to disclose, delay, modify, or destroy information handled by the IS.

b. The OIG, DoD, will have sufficient internal procedures to ensure the protection of magnetic and optical media. Where national security information is stored on removable media, controls will include measures to detect and deter removal of such media from Government control. Individuals who safeguard, control, or duplicate optical and high-density media storing a minimum of one gigabyte of information shall be designated ADP I personnel and investigated as defined in reference k.

c. Transmission of national security information shall be over communications lines meeting requirements of reference p.

## 9.7. Personnel Security

a. Personnel security clearances and access authorizations must be commensurate with the mode of operation.

b. Except in the system high and multilevel modes, users may not be granted access where they have no need-to-know for national security information contained in the system.

c. Hardware and software maintenance personnel, including vendors, must meet personnel security clearance and investigative requirements of reference k.

**9.8. Accountability, Marking, and Control of IS Media.** IS media, such as tapes, diskettes, and optical and hard disks, are documents with properties requiring additional controls to compensate for their ability to retain information, their portability and the quantity of information stored on them. Accountability and control of media shall be consistent with the highest level of national security information ever recorded on the media until the information on the media, or the media itself, is declassified. Media containing only unclassified but sensitive information are not accountable and may be released from controls when the information no longer is sensitive or is overwritten three times with random characters or a repeating pattern. The pattern must be checked by two competent individuals sector by sector to ensure no classified markings or information is apparent in any of the

sectors of the disk. Once verification has been made, a memorandum will be prepared to indicate the media no longer contains classified information and the names of the individual who verified the verification process. The memorandum will remain on file for 5 years.

a. IS media shall be marked and identified with appropriate SF Labels: SF 706, SF 707, SF 708, SF 709, SF 710, and SF 711 (see Figure 1, page 2-10).

b. Internal markings are required for textual material. Markings shall be applied as if the material were generated on paper.

c. Internal processing or storage of information on magnetic or optical media does not constitute reproduction, except where done for archival purposes, such as the generation of backup material, or where multiple copies of media, including paper copies, are made by an IS.

**9.9. Storage Media Review.** IS storage media will be reviewed periodically for information that is no longer required or authorized for retention. A three-time overwrite of such material is adequate to ensure that the information is not accessible by users with at least the requisite personnel security clearance. Such information is recoverable and the media will be retained under control equal to the highest classification level ever processed on the media.

## 9.10. Violations and Compromises

a. Violations and compromises of classified information via an IS shall be reported immediately to the OIG Security Division using the notification procedures previously outlined in this Manual. The OIG Security Division will notify the CIO.

b. The CIO will ensure adequate procedures are instituted to facilitate compromise recovery for national security information to mitigate damage and identify information should the media or system be subject to loss or compromise. Sufficient system records, such as backup media and audit records, must be maintained to reconstruct material.

# CHAPTER 10
# NORTH ATLANTIC TREATY ORGANIZATION (NATO) CLASSIFIED INFORMATION

**10.1. NATO Classified Information.** The OIG Security Division has established control points to provide a centralized location for the control, accountability, distribution, and limited destruction of NATO documents. Each control point will:

a. Stamp NATO Confidential documents "Retain or Destroy As Required." Such documents will be distributed to control points without a signature.

b. Maintain tracer action capability for all NATO Secret documents.

c. Attach a Top Secret document record (or suitable form), to each COSMIC/ATOMAL document upon initial receipt. Coordinate the receipt and control of the document with the TSCO.

d. Attach an appropriate cover sheet and stamp the word "NATO" thereon.

e. Maintain COSMIC/ATOMAL destruction certificates. Document receipts and destruction certificates, control records, disclosure records, and external transfer receipts affecting permanent transfer for these records must be retained in accordance with records management procedures.

f. Furnish the OIG Security Division with a current roster with authentication of signature card(s) for all NATO/ATOMAL control officers and alternates. The roster will be updated annually or when changes occur. These personnel will be required to receive an annual NATO briefing.

g. Destroy all NATO documents up to Secret and complete destruction certificates for NATO Secret documents. (Two NATO Secret cleared individuals must sign the destruction certificate. At least one person assigned to burn detail shall be NATO/Secret cleared.) Retain the original destruction certificate for a minimum of 5 years.

h. File destruction records for NATO documents separately from those for U.S. documents.

i. Store NATO documents in the same approved security container for non-NATO material provided they are separated by a file divider.

j. Keep an up-to-date record of individuals having custody of COSMIC/ATOMAL and NATO Secret documents in their charge. The OIG, DoD, personnel having access to NATO information must be briefed annually.

k. Ensure that the combination to a security container containing NATO documents is changed annually.

l. Conduct a 100 percent inventory of COSMIC Top Secret documents reflecting accountability, as of December 31 of each year.

m. Be aware of those individuals briefed for NATO access and ensure that uncleared personnel are not given access to NATO information or to the container in which the information is stored.

# CHAPTER 11
# PROGRAM MANAGEMENT

**11.1. General Management.** Supervisors at all OIG component levels are responsible for effective program implementation and are accountable for the security performance of their employees.

**11.2. Program Monitoring.** The OIG Security Division is responsible for monitoring, inspecting, with or without prior announcement, or conducting staff assistance visits at locations involved in classified activities. Written documentation of inspections and staff assistance visits shall be maintained and available for review for a minimum of 2 years. Counterintelligence technical inspections will be conducted or scheduled by the OIG Security Division on an "as needed" or recurring basis. The OIG Security Division will:

a. Demonstrate personal commitment and commit senior management to the successful implementation of the program established under reference a.

b. Promulgate implementing instructions.

c. Establish and maintain security education and training programs.

d. Establish and maintain an on-going self-inspection program, which shall include the periodic review and assessment of OIG, DoD, classified products.

e. Establish procedures to prevent unnecessary access to classified information, including procedures that:

(1) Require that a need for access to classified information be established before initiating administrative clearance procedures.
(2) Ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.
(3) Develop special contingency plans to safeguard classified information used in or near hostile or potentially hostile areas.
(4) Assure that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the employee's rating.
(5) Account for the costs associated with the implementation of reference a, which shall be reported to the Director of ISOO for publication.
(6) Promptly assign OIG, DoD, personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of reference a that pertains to classified information that originated in an OIG component that no longer exists and for which there is no clear successor in function.

**11.3. Field Program Management.** The OIG, DoD, field activities; shall appoint, in writing, an official to serve as security manager for the activity. To ensure compliance with this Manual, this official shall be responsible for the administration of an effective information security program emphasizing security education and training; assignment of proper classification, downgrading, and declassification; and overall information security oversight.

**11.4. Appointing Authorities** shall ensure that officials appointed as component security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They shall provide sufficient resources of time, staff and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of

the Information Security Program at all levels of the activity. (Appointing authorities include OIG Component Heads and Special Agents In Charge of the field activities.)

**11.5. Appointed Security Managers** serve as a focal point for the OIG component for advice and assistance and distribution of OIG, DoD, policy on classification, declassification, downgrading, and marking of national security information. They will conduct and coordinate the following actions with the OIG Security Division:

a. Conduct annual self-inspections of their security programs.

b. Prepare a Standard Operating Procedure (SOP) for unique situations in their OIG component that have not been addressed in this Manual. (The SOP must be submitted to the OIG Security Division for approval before implementation in the OIG component.)

c. Ensure that indoctrination, refresher, threat, courier, foreign travel, and termination briefings are conducted. Maintain an official file copy of the orientation and annual briefings. Attendance verification can be obtained through the OIG Security Division.

d. Ensure a periodic document review program is conducted in the OIG component annually to reduce unnecessary classified holdings. The program will include downgrading, declassifying, destroying, or returning documents to originator.

e. Report all security incidents or violations to the OIG Security Division and serve as the point of contact on the status of ongoing preliminary inquiries and/or formal investigations.

f. Prepare and/or coordinate requests for badges and designation letters.

g. Coordinate DD Forms 1610, *Request and Authorization for TDY Travel of DoD Personnel*, as necessary, acknowledging that travelers are authorized to hand carry classified material and have received a briefing before departure regarding applicable export control, foreign disclosure, and security requirements.

h. Maintain an account for all classified information stored, handled, and processed in their components.

# CHAPTER 12
# BUILDING ENTRANCE POLICY/BADGES/PROPERTY PASSES/ESCORTING

**12.1. Policy**. Only authorized personnel with a valid DoD identification (ID) are allowed access into 400 Army Navy Drive. All other personnel must sign in and be escorted. Café patrons will be permitted to walk through the lobby to the café. Personnel working at off-site field activities must ensure visitors are properly cleared and SOPs address visitor control, property removal, and deliveries. Visitors will be controlled and escorted in OIG, DoD, offices located in Crystal Gateway North.

a. Acceptable ID (Building Passes)

(1) White DoD Badge (DoD Employees)
(2) Pink DoD Badge (Contractors)
(3) Blue DoD Badge (Press/Foreign Nationals)
(4) Gray (Retired DoD Civilians)
(5) Tan Temporary (Press)
(6) DoD Civilian ID
(7) Military ID

b. X-ray and Metal Detector Screening. Individuals without an acceptable ID badge must go through the metal detector screening. Packages in their possession must also be screened through the x-ray machine. Packages too large for screening will be physically checked.

c. Mail/FEDEX/UPS/RPS/Airborne Deliveries. Packages will go through the x-ray machine for screening. To avoid problems with the lobby guards, delivery personnel should have a designated point of contact. Delivery personnel should at least know the office to where the package is to be delivered. Packages will not be dropped off at the guard desk or held by the lobby guards.

d. Bulk Deliveries (Supplies and Equipment, etc.). Bulk deliveries that are expected and verified do not require screening. The escort will be responsible for the shipment.

e. Removing Property. Property (including personal property) being removed from 400 Army Navy Drive must be accompanied by a valid Property Pass (Optional Form 7) (Figure 19, page 12-4). Lobby guards will check the serial number, bar code, and description of the item to verify that it corresponds to the information listed on the property pass.

f. Exceptions may be granted to waive visitor badge and X-ray screening on a case-by-case basis. Advance coordination must be made with the OIG Security Division to have these requirements waived.

g. Before and After Hours Sign-In. For safety reasons, OIG, DoD, personnel are required to sign-in before 6:00 a.m. and after 6:00 p.m. during weekdays. Additionally, personnel will sign in and out during weekends and holidays.

h. Forgotten or Lost Badges. Employees who forget or lose their badge may be issued a temporary badge by the main lobby guards at 400 Army Navy Drive. A personnel roster of all DoD civilian employees is maintained at the front lobby desk. Military personnel may show a military ID to gain entry and to obtain a temporary badge. Temporary badges issued to the individual will require an exchange ID or drivers license. The ID or driver license will be returned to the individual when the temporary ID is returned to the main lobby guard desk. Lost or broken badges may be replaced by going directly to the Pentagon Building Pass Office. Expired badges must be taken to the OIG Security Division for renewal.

**12.2. Basic Rules for Escorting and General Escort Requirements.** The escort must accept responsibility for the uncleared individuals visiting OIG, DoD, facilities. By doing so, the escort acknowledges his or her commitment to the escort assignment, is knowledgeable of escorting requirements and guidelines, and assumes control over the visitor at all time. The escort must be familiar with the OIG Fire and Building Evacuation Plan and know what to do in case of an evacuation procedure. The escort must observe all security rules and regulations and will ensure uncleared individuals comply with OIG, DoD, instructions and directions. The need-to-know rule applies to all persons at all times. The escort must maintain visual contact with escorted personnel at all times and/or must be in a position to control the movement and actions of uncleared persons. The escort must remain with visitors at all times until he/she is turned over to another official or escort; or leaves the OIG, DoD, facility. Escorts must ensure that the uncleared person(s) wears his or her badge above the waist.

a. Non-OIG personnel, workers, contractors, maintenance personnel, and delivery personnel cannot perform escort responsibilities. Exceptions to this rule must be addressed individually with the OIG Security Division.

b. Escorting Groups. When escorting a group, the limit ratio is one escort to not more than 5 uncleared persons--all within the line of sight.

c. Office Areas. When escorting individuals into an office area (or any processing area), the escort will ensure that:

(1) Repositories are locked or drawers closed.
(2) No classified data is visible on a computer screen.
(3) No classified documents are unattended.
(4) Persons using classified material are advised to shield such information.
(5) No classified discussions are held in the presence of uncleared personnel.
(6) Reproduction machines, telefax, secured telephones, and mail drops are free of visible classified data.
(7) Be aware of the movement of classified materials through areas where uncleared visitors are present.
(8) Needs to be aware of what items are placed in all toolboxes.

**12.3. Escorting Persons with a Suspended Clearance or Restricted Access.** The OIG, DoD, employees whose clearances are suspended will be escorted at all times. Escorts will ensure that they are in full compliance with this Manual.

**12.4. Non-receipt of Visit Certification Letter.** Visitors occasionally arrive at OIG, DoD, facilities without having had their security clearance passed by their security office. Although the escort may have personal knowledge that the visitor holds a clearance at another facility, or they tell you their clearance is held elsewhere, or they show you their facility badge, they must still be treated as uncleared. A security badge can only grant access to areas in OIG, DoD, facilities. A “security badge” will not be used to grant an individual access to classified information.

**12.5. Field Activity Managers and OIG Components.** The OIG components and field activity managers are responsible for classified information security within their areas. Therefore, managers who request uncleared personnel be afforded access to their areas are certifying that appropriate security measures are in place, that uncleared personnel will not be afforded access to classified matter and that escorts are properly briefed.

**12.6. <u>Challenges</u>.** Should any OIG, DoD, employee observe an uncleared individual unescorted, it is the employee's responsibility to become an escort to that person. This may be accomplished by detaining the uncleared person while you call the OIG Security Division or front lobby guards to respond to your location or to escort the individual to the front lobby guard desk. Uncleared employees who observe an unescorted individual should report the situation to their escort who will take appropriate action. ***The OIG, DoD, personnel should never ignore the situation – each OIG, DoD, employee is authorized and obligated to take immediate action.***

OPTIONAL FORM 7
SEPTEMBER 1988
PRESCRIBED BY GSA
FPMR (41 CFR) 101–20.110

# PROPERTY PASS

1. DATE ISSUED

This pass is to be used whenever property is removed from the building. It is to be properly filled in and signed and handed to the guard when leaving the building.

2. NAME

3. BUILDING

4. DESCRIPTION OF PROPERTY BEING REMOVED

5. PROPERTY BELONGS TO

6. DEPARTMENT OR AGENCY

7. SIGNATURE OF PERSON AUTHORIZING REMOVAL OF PROPERTY

8. TITLE

9. PASS GOOD UNTIL

NSN 7540–00–634–4264 *U.S. Government Printing Office: 1993 — 300-892/60168 5007–105

Figure 19. Sample Optional Form (OF) 7, Property Pass

# CHAPTER 13
# OIG SELF INSPECTION PROGRAM

| **ALL PURPOSE CHECKLIST** | | **PAGE 1 OF 7 PAGES** | | |
|---|---|---|---|---|
| **TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA**<br>Information Security Self-Inspection Checklist | | **OIG COMPONENT** | **DATE** | |
| NO. | **ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*** | YES | NO | N/A |
| | **PROGRAM MANAGEMENT** | | | |
| 1. | Has the each OIG Component Head appointed a security manager to oversee the implementation and oversight of the provisions of DoD 5200.1-R? (DoD 5200.1-R, Ch 1, section 2, para 1-201c) | | | |
| 2. | Did the OIG component develop and implement, through the security manager, security instructions necessary for program implementation? (DoD 5200.1-R, Ch.1, Section 2, para 1-202b) | | | |
| 3. | Does the security manager host a staff assistance visit with the OIG Security Division | | | |
| 4. | Does the OIG component security manager attend the Security Manager's Working Group (SMWG) training sponsored by the OIG Security Division? (DoD 5200.1-R, Ch 9, para. 9-300) | | | |
| 5. | Does the OIG component security manager notify personnel when training classes are being held by the OIG Security Division? | | | |
| 6. | Does the security manager oversee the conduct of his/her component security inspections (self-inspection)? (DoD 5200.1-R, Ch. 1, Section 7, para 1-7) | | | |
| | • Is the OIG Component Head informed of the results of such inspections? | | | |
| 7. | Does the OIG Security Division implement and maintain an effective security education program as required by DoD 5200.1-R, Chapter 9, to include initial orientation and continuing/refresher training for assigned employees? (DoD 5200.1-R, Ch 1, Section 2, para 1-200(a) and section 4, para 9-400 and 401) | | | |
| 8. | Do the OIG component security managers and the OIG Security Division document all security-related training? (DoD 5200.1-R, Ch 9, Section 5, para 9-600) | | | |
| 9. | Are procedures established to prevent unauthorized access to classified information? (DoD 5200.1-R, Ch 1, Section 2, para 1-202(e)) | | | |
| | • Note: Examples include implementing visitor controls, restricting combinations to cleared members, establishing end-of-day security checks, etc) | | | |
| 10. | Are employees familiar with the procedures for safeguarding classified information in case of fire, natural disaster or civil disturbance? | | | |
| 11. | Are procedures established to ensure that all persons handling classified material are properly cleared and have a need-to-know? (DoD 5200.1-R, Section 1, para 1-101e) | | | |
| 12. | Does the OIG Security Division and OIG component security manager maintain a continuity handbook? (DoD 5200.1-R, Section 2, para 1-202) | | | |

| ALL PURPOSE CHECKLIST | | PAGE 2 OF 7 PAGES | | |
|---|---|---|---|---|
| **TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA**<br>Information Security Self-Inspection Checklist | | **OIG COMPONENT** | **DATE** | |
| NO. | **ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*** | YES | NO | N/A |
| | **CLASSIFICATION MANAGEMENT** | | | |
| 1. | Is information classified only if it concerns one of the categories specified in Section 1.5 of Executive Order 12958: military plans, weapon systems or operations; foreign government information, intelligence sources or methods, or cryptology; scientific, technological or economic matters; or vulnerabilities or capabilities of systems? | | | |
| | **DOCUMENT MARKING** | | | |
| 1. | Are derivatively classified documents properly marked when information is extracted from a classified source, to include the: | | | |
| | • Overall classification (DoD 5200.1-R, Ch 5, para 5-200) | | | |
| | • The agency, office or origin, and date (DoD 5200.1-R, Ch 5, para 5-201) | | | |
| | • A "Derived From:" line (DoD 5200.1-R, Ch 5, para 5-202b) | | | |
| | • Identification of the "sources" of classification (DoD 5200.1-R, Ch 5, para 5-202(b)2) | | | |
| | • Declassification instructions (DoD 5200.1-R, Ch 5, para 5-204c) | | | |
| | • Downgrading instructions, if required (DoD 5200.1-R, Ch 5, para 5-205) | | | |
| | • Page markings (DoD 5200.1-R, Ch 5, para 5-207) | | | |
| 2. | Are "subjects" or "titles" of classified documents marked with the appropriate symbol (TS), (S), (C), or (U) following and to the right of the title or subject? (DoD 5200.1-R, Ch 5, para 5-206(a)2) | | | |
| 3. | Is each section, part, paragraph or similar portion of a classified document marked to show the highest level of classification of information it contains, or that it is unclassified? Portions of text shall be marked with the appropriate abbreviations (TS, S, C, or U). (DoD 5200.1-R, Ch 5, para 5-206a) | | | |
| 4. | Are portions within documents containing Restricted Data and Formerly Restricted Data marked with the abbreviation "RD" or "FRD" (e.g., S-RD or TS-FRD)? (DoD 5200.1-R, Ch 5, para 5-206a1a) | | | |
| 5. | Are portions within documents containing foreign government or North Atlantic Treaty Organization (NATO) information marked with the foreign classification or N for NATO with the appropriate level (e.g., UK-S or N-TS)? (DoD 5200.1-R, Ch 5, para 5-206a1b) | | | |
| 6. | Is the abbreviation "FOUO" used to designate unclassified portions that contain information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)? (DoD 5200.1-R, Ch 5, para 5-206a1c, and Appendix C) | | | |
| 7. | Are charts, graphs, photographs, illustrations, figures and similar items within classified documents marked to show their classification? (DoD 5200.1-R, Ch 5, para 5-206a3) | | | |
| 8. | Are the markings placed within the chart, graph, photograph, illustration, figure, etc. or next to the item? (DoD 5200.1-R, Ch 5, para 5-2063b) | | | |

| **ALL PURPOSE CHECKLIST** | | **PAGE** 3 **OF** 7 **PAGES** | | |
|---|---|---|---|---|
| **TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA**<br>Information Security Self-Inspection Checklist | | **OIG COMPONENT** | **DATE** | |
| NO. | **ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*** | YES | NO | N/A |
| 9. | Is the highest classification level placed on the top and bottom of each page containing classified information or marked "unclassified"? | | | |
| 10. | Do the markings stand out from the balance of the information on the page (must be readily visible)? (DoD 5200.1-R, Ch 5, para 5-207) | | | |
| 11. | Are TRANSMITTAL documents properly marked to include either the highest classification or a notation "Unclassified when separated from classified enclosures"? (DoD 5200.1-R, Ch 5, para 5-301) | | | |
| 12. | For ELECTRONICALLY transmitted documents: | | | |
| | • Is the FIRST item in the text the overall classification? (DoD 5200.1-R, Ch 5, para 5-304a) | | | |
| | • Is the overall and page marking applied conspicuously to each page? (DoD 5200.1-R, Ch 5, para 5-304b) | | | |
| | • Does the LAST line include a "Classified by:" or "Derived From:" line and declassification and downgrading instructions? (DoD 5200.1-R, Ch 5, para 5-304c) | | | |
| 13. | Are files, folders, and groups of documents clearly marked on the outside of the file or folder (attaching a classified document cover sheet to the front of the folder or holder will satisfy this requirement)? (DoD 5200.1-R, Ch 5, para 5-306) | | | |
| 14. | Are removable storage media (e.g. magnetic tape reels, disk packs, diskettes, CD-ROMS, removable hard disks, disk cartridges, tape cassettes, etc.) marked with the appropriate Standard Form label (SF 706/707/708/709/ 710)? (DoD 5200.1-R, Ch 5, para 5-407/409) | | | |
| | **SAFEGUARDING AND STORAGE** | | | |
| 1. | Is classified information removed from storage kept under constant surveillance of authorized persons? (DoD 5200.1-R, Ch 6, para 6-301) | | | |
| 2. | Are cover sheets placed on all documents removed from storage? (DoD 5200.1-R, Ch 6, para 6-301a) | | | |
| 3. | Are end-of-day security checks established for areas that process or store classified information to ensure the area is secure at the close of each working day? (DoD 5200.1-R, Ch 6, para 6-302 ) | | | |
| 4. | Is the SF 701, Activity Security Checklist, used to record end-of-day checks? (DoD 5200.1-R, Ch 6, para 6-302) | | | |
| 5. | Is the SF 702, Security Container Check Sheet, used to record the closing of each vault, secure room or container used for storage of classified material? (DoD 5200.1-R, Ch 6, para 6-302) | | | |
| 6. | Is the SF 700, Security Container Information, properly completed and posted inside the LOCKING drawer of the security container, or inside the door of vault and similar facilities? (DoD 5200.1-R, Ch 6, para 6-404b3) | | | |
| 7. | Are storage containers (safes) that may have been used to store classified information inspected by properly cleared personnel before removal from protected areas or before unauthorized persons are allowed access to them? (DoD 5200.1-R, Ch 6, para 6-305) | | | |

| **ALL PURPOSE CHECKLIST** | | **PAGE 4 OF 7 PAGES** | | |
|---|---|---|---|---|
| **TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA**<br>Information Security Self-Inspection Checklist | | **OIG COMPONENT** | **DATE** | |
| NO. | **ITEM**<br>***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*** | YES | NO | N/A |
| 8. | Are combinations to security containers changed at the required intervals? (DoD 5200.1-R, Ch 6, para. 6-404b) | | | |
| 9 | If written records of the combination are maintained, are they marked and protected at the highest classification of the material stored therein? (DoD 5200.1-R, Ch 6, para 6-404b2) | | | |
| 10. | • Is the combination stored in a security container other than the one for which it is being used? | | | |
| 11. | Are entrances to secure rooms or areas under visual control at all times during duty hours to prevent unauthorized access or equipped with electric, mechanical or electromechanical access control devices to limit access during duty hours? (DoD 5200.1-R, Ch 6, para 6-404b) | | | |
| 12. | Does each vault or container bear an external marking for identification purposes? NOTE: The level of classification stored therein must NOT be marked on the outside of the container(s). (DoD 5200.1-R, Ch 6, para 6-404) | | | |
| 13. | Is Top Secret material stored only in a GSA-approved security container having one of the following supplemental controls: (DoD 5200.1-R, Ch 6, para 6-402a) | | | |
| | • Continuous (24 hour) protection by cleared guard or duty personnel | | | |
| | • Cleared guard or duty personnel inspect the security container every 2 hours | | | |
| | • An Intrusion Detection System (Alarm System) meeting requirements of a 15 minute response time. (SCIF areas DCID 1/19) | | | |
| | • Combination lock meeting Federal Specification FF-L-2740 (XO-7) with Security-In-Depth | | | |
| 14. | Is Secret material stored in a GSA-approved security container (safe) without supplemental controls or in the same manner as Top Secret? (NOTE: Approved containers will have a certification label on the container itself.) (DoD 5200.1-R, Ch 6, para 6-402b) | | | |
| 15. | Is Confidential material stored in a GSA-approved security container? (DoD 5200.1-R, Ch 6, para 6-402c) | | | |
| 16. | Are security container repairs (e.g. drilled because of a forgotten combination) done in accordance with DoD 5200.1-R, Ch 6, para 6-405? | | | |
| 17. | Do activity security procedures prescribe appropriate safeguards for Information Processing Equipment (IPE)--specifically: (DoD 5200.1-R, Ch 6, para 6-309 a/b/c) | | | |
| 18. | Is IPE, e.g., copiers, facsimile machines, AIS equipment and peripherals, electronic typewriters and word processing systems, used for processing classified information protected from unauthorized access? (DoD 5200.1-R, Ch 6, para 6-309a) | | | |
| 19. | Do appropriately cleared and technically knowledgeable personnel inspect the IPE before the equipment is removed from the protected areas? (DoD 5200.1-R, Ch 6, para 6-309c) | | | |

| ALL PURPOSE CHECKLIST | | PAGE 5 OF 7 PAGES | | |
|---|---|---|---|---|
| TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA<br>Information Security Self-Inspection Checklist | | OIG COMPONENT | DATE | |
| NO. | ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)* | YES | NO | N/A |
| 20. | Are GSA-approved field safes and special purpose one and two-drawer lightweight security containers securely fastened to the structure or under sufficient surveillance to prevent their theft? (DoD 5200.1-R, Ch 6, para 6-402d2) | | | |
| | **REPRODUCTION OF CLASSIFIED MATERIAL** | | | |
| 1. | Are procedures established to limit the reproduction of classified material? (DoD 5200.1-R, Ch 6, para 6-500 ) | | | |
| 2. | Are personnel who reproduce classified material aware of the risks involved with the specific reproduction equipment and the appropriate counter-measures they are required to take? (DoD 5200.1-R, Ch 6, para 6-502c) | | | |
| 3. | Are waste products generated during reproduction properly protected and disposed of? (DoD 5200.1-R, Ch 6, para 6-502f) | | | |
| 4. | Is reproduction equipment specifically designated for the reproduction of classified material? (DoD 5200.1-R, Ch 6, para 6-502b) | | | |
| 5. | Are RULES POSTED on or near the designated equipment authorized for the reproduction of classified? (DoD 5200.1-R, CH 6, para 6-502) | | | |
| 6. | Are NOTICES prohibiting reproduction of classified material POSTED on equipment used only for the reproduction of unclassified material? (DoD 5200.1-R, Ch 6, Section 5) | | | |
| | **DISPOSITION AND DESTRUCTION OF CLASSIFIED MATERIAL** | | | |
| 1. | Are documents that are no longer required for operational purposes disposed of in accordance with the provisions of the Federal Records Act (44 U.S.C., Chapters 21, 31, and 33) and appropriate implementing directives and records schedules? (DoD 5200.1-R, Ch 6, para 6-700) | | | |
| 2. | Has each activity with classified holdings set aside at least one "Clean-Out" day each year when specific attention and effort is focused on disposition of unneeded classified material? (DoD 5200.1-R, Ch 6, para 6-700b) | | | |
| 3. | Is classified material properly destroyed by approved methods? (DoD 5200.1-R, Ch 6, para 6-701a) | | | |
| | **TRANSMISSION AND TRANSPORTATION OF CLASSIFIED INFORMATION** | | | |
| 1. | Whenever classified information is transmitted outside of the activity, is it enclosed in two opaque sealed envelopes or similar wrappings or containers durable enough to properly protect the material from accidental exposure and facilitate detection of tampering? (DoD 5200.1-R, Ch 7, para 7-200) | | | |
| | • NOTE: When classified material is hand carried outside an activity, a locked briefcase may serve as the outer wrapper. | | | |
| 2. | Is the outer wrapper addressed to an official Government activity or to a DoD contractor with a facility clearance and appropriate storage capability with a complete return address of the sender? (DoD 5200.1-R, Ch 7, para 7-201a) | | | |

| ALL PURPOSE CHECKLIST | | PAGE 6 OF 7 PAGES | | |
|---|---|---|---|---|
| **TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA**<br>Information Security Self-Inspection Checklist | | **OIG COMPONENT** | **DATE** | |
| NO. | **ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*** | YES | NO | N/A |
| 3. | Is the inner wrapper or container marked with the following information: sender's and receiving activity's address and highest classification level of the contents (including where appropriate, any special markings) | | | |
| | • NOTE: The inner envelope may have an "attention line" with a person's name. (DoD 5200.1-R, Ch 7, para 201b) | | | |
| 4. | Are procedures established to limit hand carrying classified information to only when other means of transmission or transportation cannot be used? (DoD 5200.1-R, Ch 7, para 7-300a) | | | |
| 5. | Are hand carrying officials briefed on and have they acknowledged their responsibilities for protecting classified information? (DoD 5200.1-R, Ch 7, para 7-300b) | | | |
| | **TRANSMISSION AND TRANSPORTATION OF CLASSIFIED INFORMATION (CONT)** | | | |
| 1. | Are courier officials provided a written statement authorizing such hand carrying transmission? (DoD 5200.1-R, Ch 7, para 7-301a) | | | |
| | • Does the activity list all classified carried or escorted by traveling personnel? (DoD 5200.1-R, Ch 7, para 7-300b(8)c) | | | |
| | • Does the activity keep this list until all material reaches the recipient's activity? (DoD 5200.1-R, Ch 7, para 7-300b(8(d) | | | |
| 2. | Is the DD Form 2501, Courier Authorization Card, controlled to preclude unauthorized use? (DoD 5200.1-R, Ch 7, para 7-301(b)3 ) | | | |
| 3. | Do courier officials coordinate in advance with airline and departure terminal officials to develop mutually satisfactory arrangements in accordance with this regulation and Federal Aviation Administration (FAA) guidance before hand carrying classified materials aboard "commercial" airlines? (DoD 5200.1-R, Ch 7, para 7-302) | | | |
| 4. | When "Confidential" classified information is sent via U.S. Postal Service "First Class" mail between DoD components within the United States, is the outer envelope or wrapper endorsed "POSTMASTER: Return Service Requested; Do Not Forward"? (DoD 5200.1-R, Ch 7, para 7-103d ) | | | |
| 5. | Do recipients of first class mail bearing the "Postmaster" notice protect it as Confidential material? | | | |
| | **SECURITY EDUCATION** | | | |
| 1. | Does the OIG component support the OIG Security Education Program? How many personnel from the OIG component attended versus did not attend? (DoD 5200.1-R, Ch 9) | | | |
| 2. | Does the OIG training program include an "initial orientation" for all assigned personnel who are cleared for access to classified information? (DoD 5200.1-R, Ch 9, para 9-200a ) | | | |
| 3. | Does this orientation include the: (DoD 5200.1-R, Ch 9, para 9-200a(1)(2)(3) | | | |
| | • Roles and responsibilities of assigned members and essential personnel? | | | |
| | • Elements of safeguarding classified information? | | | |
| | • Elements of classifying and declassifying Information? | | | |
| | • Will be traveling to foreign countries? | | | |

| **ALL PURPOSE CHECKLIST** | | **PAGE 7 OF 7 PAGES** | | |
|---|---|---|---|---|
| **TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA** Information Security Self-Inspection Checklist | | **OIG COMPONENT** | **DATE** | |
| NO. | **ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*** | YES | NO | N/A |
| 4. | Are training programs established for employees who: (DoD 5200.1-R, Ch 9, para 9-304) | | | |
| | • Will be traveling to foreign countries? | | | |
| | • Will be escorting, hand carrying or serving as a courier for classified material? | | | |
| | • Will use automated information systems to store, process or transmit classified? | | | |
| 5. | Is refresher training provided at least annually to assigned employees? (DoD 5200.1-R, Ch 9, para 9-401) | | | |
| 6. | Is refresher training tailored to the mission needs and address policies, principles and procedures covered in initial training? (DoD 5200.1-R, Ch 9, para 9-401) | | | |
| 7. | Does refresher training address concerns identified during component self-inspections? (DoD 5200.1-R, Ch 9, para 9-401) | | | |
| 1. | Are procedures established to ensure cleared employees who leave the organization or whose clearance is terminated receive a termination briefing? (DoD 5200.1-R, Ch 9, para 9-500) | | | |
| 2. | Are records maintained to show the names of employees who participated in "initial" and "refresher" training? (DoD 5200.1-R, Ch 9, para 9-600 ) | | | |
| 3. | Do training programs for "uncleared" employees include: | | | |
| | • The nature and importance of classified information? | | | |
| | • Actions to take if they discover classified information unprotected? | | | |
| | • The need to report suspected contact with a foreign intelligence collector? | | | |
| | **SECURITY INCIDENTS AND VIOLATIONS, TO INCLUDE COMPROMISES** | | | |
| 1. | Are assigned employees aware of their responsibilities to report security violations concerning classified information? (DoD 5200.1-R, Ch 10, para 10-101b) | | | |
| 2. | Do security managers report security incidents and violations to the OIG Security Division | | | |
| 3. | Is an inquiry and/or investigation promptly conducted to ascertain the facts surrounding a reported incident? (DoD 5200.1-R, Ch 10. para 10-102) | | | |

# APPENDIX A
# REFERENCES

a. Executive Order (E.O.) 12958, “Classified National Security Information,” April 20, 1995, effective October 14, 1995

b. DoD 5200.1-R, "Information Security Program Regulation," January 17, 1997

c. DoD 5200.1-PH, "DoD Guide to Marking Classified Documents," April 1997

d. DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 1998

e. Title 5, U.S.C., Section 522, as amended (Public Law 104-231, 110 stat.2422) The Freedom of Information Act

f. Title 5, U.S.C., Section 522a (Public Law 93-579), The Privacy Act of 1974

g. Title, 44, U.S.C., Chapters 21, 31, and 33, Federal Records Act

h. DoD Directive 5210.56, "Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties," February 25, 1992

i. DoD Directive 3224.3, "Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support," February 17, 1989

j. Title 18, U.S.C., Section 1386, Crimes and Criminal Procedure, 1982

k. DoD 5200.2-R, "Personnel Security Program," January 1987

l. DoD Instruction O-5230.22, "Security Controls on the Dissemination of Intelligence Information," August 17, 1988

m. DoD Directive 5200.33, "Defense Courier Service (DCS)," January 5, 1995

n. DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

o. DoD Directive 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

p. DoD Directive C-5200.5, "Communications Security (COMSEC)," April 21, 1990

# APPENDIX B
# DEFINITIONS

The following definitions are commonly used throughout the intelligence/security community. These definitions are provided for easy reference. The definitions may or may not appear in this Manual. The definitions are meant to aid the user when such terminology is used in conversation or written correspondence.

a. **Access**. The ability or opportunity to gain knowledge of classified information.

b. **Accreditation**. A formal declaration by the Designated Approving Authority (DAA) that the Information System (IS) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an IS and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

c. **Agency**. Any "Executive Agency," as defined in 5 United States Code (U.S.C.) 105, and any other entity within the executive branch that comes into the possession of classified information.

d. **Automatic Declassification**. The declassification of information based solely upon:

1. The occurrence of a specific date or event as determined by Original Classification Authority (OCA); or

2. The expiration of a maximum period for duration of classification established under reference a.

e. **Automated Information System (AIS) or Information System**. An assembly of computer hardware, software or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

f. **Certification**. (Also called **Functional Compliance Certification**, **Security Certification** and **Summary Certification**). The technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which established the extent that a particular AIS's design and implementation meets a set of specified security requirements.

g. **Classification**. The act or process by which information is determined to be classified information.

h. **Classification Guidance**. Any instruction or source that prescribes the classification of specific information.

i. **Classification Guide**. A documentary form of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

j. **Classified Contract**. Any contract that requires or will require access to classified information by the contractor or contractor employees in the performance of the contract. A contract may be classified although the contract documentation is not classified.

k. **Classified National Security Council (NSC) Information** (hereafter called NSC Information). Classified information contained in documents prepared by or for the NSC, its interagency groups and associated committees and groups. The term also includes deliberations of the NSC, its interagency groups and associated committees and groups.

l. **Classified National Security Information** (hereafter "classified information"). Information that has been determined following reference a or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

m. **Cleared Contractor Facility**. A contractor facility in the United States that has been granted a facility security clearance in accordance with the National Industrial Security Program. The level of clearance granted to individual facilities varies.

n. **Confidential Source**. Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

o. **Contact Officer**. An OIG, DoD, official designated in writing to oversee and control the activities of foreign representatives accredited to or visiting OIG, DoD, facilities.

p. **Damage to the National Security**. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

q. **Declassification**. The authorized change in the status of information from classified information to unclassified information.

r. **Declassification Authority**:

1. The official who authorizes the original classification, if that official is still serving in the same position.

2. The originator's current successor in function.

3. A supervisory official of either 1 or 2 above.

4. Officials delegated declassification authority in writing by the Inspector General, DoD, or his or her designee.

s. **Declassification Guide**. Written instructions issued by a declassification authority that describe the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

t. **Derivative Classification**. The incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly created material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

u. **Downgrading**. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

v. **Extended Visit**. Identical to a visit, except that approval is extended for recurring contacts over a longer time, normally not to exceed 1 year.

w. **File Series**. Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

x. **Foreign Disclosure**. The conveying of classified information to an authorized representative of a foreign government or international organization in a manner approved by this Manual. It may be accomplished by providing documents or materials or by oral or visual means, including briefings, conferences, or other meetings.

y. **Foreign Government Information**:

1. Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence.

2. Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

3. Information received and treated as "Foreign Government Information" under the terms of a predecessor order.

z. **Foreign Nationals**. All persons who are not citizens, nationals, or immigrant aliens of the United States.

aa. **Foreign Representatives**. Foreign nationals as well as citizens or nationals of the United States or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official, or as a corporate employee who personally is involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, international organization, or foreign national.

bb. **Government Installation**. A U.S. Government facility where adequate measures for safeguarding classified information can be imposed.

cc. **Government to Government**. The approved channel for the disclosure of classified information by an authorized U.S. Government agency or representative of a foreign government or international organization.

dd. **Information**. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

ee. **Information System**. See ***Automated Information System***.

ff. **Infraction**. Any knowing, willful or negligent action contrary to the requirements of reference a or its implementing directives that does not comprise a "violation."

gg. **Integrity**. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, stored, or destroyed.

hh. **International Organization**. A duly constituted international body, civilian or military or both, having responsibility for any aspect of mutual defense, which may have a requirement for access to U.S. classified information in carrying out its assigned responsibilities; e.g., the International Staff of the North Atlantic Treaty Organization (NATO), Australia-New Zealand-United States (ANZUS), Inter-American Defense Board (IADB), Canada-U.S. Regional Planning Group, the military staffs of Supreme Headquarters Allied Powers, Europe (SHAPE), and Supreme Allied Command, Atlantic (SACLANT).

ii. **Limited Dissemination**. Restrictive controls for classified information established by an original classification authority to emphasize need-to-know protective measures available within the regular security system.

jj. **Mandatory Declassification Review**. The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of E.O. 12958.

kk. **Meeting**. A conference, seminar, symposium, exhibit, convention, or gathering conducted by an OIG, DoD, office, directorate, organizational element, a cleared contractor or an association, institute, or society, or employee whose membership includes DoD or contractor personnel, and during which DoD classified information or classified information of interest to the DoD is disclosed.

ll. **Multiple Sources**. Two or more source documents, classification guides or a combination of both.

mm. **National Security**. The national defense or foreign relations of the United States.

nn. **Need-to-know**. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information to perform or assist in a lawful and authorized governmental function.

oo. **Network**. A system of two or more computers that can exchange data or information.

pp. **Original Classification**. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

qq. **Original Classification Authority**. An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

rr. **Originating Agency**. The agency responsible for the initial determination that particular information is classified.

ss. **Safeguarding**. Measures and controls that are prescribed to protect classified information.

tt. **Security Sponsor**. An official designated by the Inspector General, DoD, or a designee, to be responsible for supervising all security aspects of classified meetings.

uu. **Self-Inspection**. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established reference a and its implementing directives.

vv. **Senior Agency Official**. The official designated by the agency head under section 5.6(c) of E.O. 12958 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

ww. **Sensitive Information**. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest of the conduct of Federal programs, or the privacy to which individuals are entitled reference f, but which has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

xx. **Source Document**. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

yy. **Special Access Program (SAP)**. A program established for a specific class of classified information that imposes safeguarding and accesses requirements that exceed those normally required for information at the same classification level.

zz. **Special Category (SPECAT)**. The term "SPECAT" is used only for electrically transmitted information identified with a specific project or subject having worldwide application and requiring security protection or handling not guaranteed by the primary security classification. Such messages must be handled by, and disseminated to, only those personnel specifically authorized such access. The term "SPECAT" is inserted by the originator immediately following the message classification and preceding the special category designator; e.g., TOP SECRET (SPECAT SIOP-ESI).

aaa. **Special Handling**. Special handling is that procedure required for safeguarding information annotated with code words, nicknames, or caveats, which restricts the dissemination of such information to approved areas or personnel.

bbb. **Sponsor**. An OIG component that has a principal interest in the subject matter of a meeting and that has accepted security sponsorship for the meeting.

ccc. **Systematic Declassification Review**. The review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. ("Archivist") to have permanent historical value in accordance with reference g.

ddd. **Telecommunications**. The preparation, transmission or communication of information by electronic means.

eee. **Unauthorized Disclosure**. A communication or physical transfer of classified information to an unauthorized recipient.

fff. **Violation**:

1. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

2. Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of reference a or its implementing directives.

3. Any knowing, willful, or negligent action to create or continue a SAP contrary to the requirements of reference a.